

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0212U007283

Державний реєстраційний номер: 0111U008680

Особливі позначки: відкрита

Дата реєстрації: 01-11-2012

II. Етап виконання ДіР

Номер етапу: 2

Назва етапу: Теоретичні та експериментальні дослідження. Узагальнення й оцінювання результатів дослідження.(Етап 2).

Початок етапу: 01.2012

Закінчення етапу: 06.2012

Вид звітнього документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Національний технічний університет України "Київський політехнічний інститут", Фізико-технічний інститут

Код за ЄДРПОУ: 02070921

Місцезнаходження:

Форма власності:

Сфера управління: Міністерство освіти і науки, молоді та спорту України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 406-81-76

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Служба зовнішньої розвідки України; військова частина К1410

Код за ЄДРПОУ: 33240845

Місцезнаходження: вул. Володимирська, 33, м. Київ, Київ, 01034, Україна

Форма власності:

Сфера управління: Служба безпеки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 0442262124

VI. Джерела, напрями та обсяги фінансування ДіР

Підстава для проведення ДіР: 52 - договір з вітчизняною організацією (органами місцевої ради, фондом, асоціацією, концерном тощо)

Напрямок фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

7713 - кошти держбюджету

Код програмної класифікації видатків і кредитування (КПКВК): 6621010

Фактичний обсяг фінансування (тис. грн.): 100
--

VII. Відомості про ДіР

Назва роботи українською:

Застосування сучасних математичних методів у криптоаналізі

Назва роботи англійською:

Application of modern mathematical methods is in kryptoanalizi.

Реферат українською:

Об'єктом дослідження НДР є системи та процеси криптографічного захисту інформації, випадкові послідовності та функції, важкооборотні перетворення в класичній та постквантовій моделі обчислень, криптоаналітичні атаки. В роботі розвинуто та узагальнено існуючі методи криптоаналізу та розроблено нові математичні моделі стійкості криптографічних систем захисту інформації і методи аналізу криптографічних алгоритмів, зокрема, симетричних блочних та поточних шифрів; оцінені їх можливості, визначено стійкі та нестійкі класи шифрів відносно криптоаналітичних атак, що розглядаються; зроблено прогнозування тенденцій розвитку сучасних методів криптоаналізу та їх впливу на методологічну базу криптології

Реферат англійською:

The object of research of work are the systems and processes of cryptographic protection of information, random sequences and functions, trapdoor functions that are considered in the classic and post-quantum model of calculations, cryptanalytic attacks. The current methods of cryptanalysis are developed and generalized, the new mathematical models of security of the cryptosystems of protection of information and methods of analysis of cryptographic algorithms are worked out, in particular, of symmetric block and stream ciphers; their possibilities are evaluated, the secure and unsecure classes of ciphers are defound in relation to considered cryptanalitic attacks; prognostication of progress of modern methods of cryptanalysis and their influence trends on the methodological base of cryptology is done.

Індекс УДК: 681.3.06:004.92, 681.3.06:519.248.681

Коди тематичних рубрик: 81.14.11.05

Керівники роботи

Власне Прізвище Ім'я По-батькові: Савчук Михайло Миколайович

Науковий ступінь:

Вчене звання:

Ідентифікатор ORCID ID:

Додаткова інформація:

VIII. Наукова (науково-технічна) продукція (НТП)

Назва НТП українською: Новы математичны методи за результатами НДР "Застосування сучасних математичних методів у криптоаналізі"

Назва НТП англійською: Scientific and technical report on the results of scientific research work "Application of modern mathematical methods in kryptoanalizi"

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати:

Галузь застосування: 73.10.1- Дослідження і розробки в галузі природничих та технічних наук

Реєстраційний номер картки технології:

Опис НТП: Науково-дослідна робота "Застосування сучасних математичних методів у криптоаналізі" (шифр "Кашалот-5"), виконувалась в 2 етапи протягом дев'яти місяців, з жовтня 2011 р. по червень 2012 р. Дана робота є продовженням НДР "Кашалот-4". Звіт по НДР висвітлює дослідження, проведені на першому та другому етапі роботи; згідно технічного завдання у звіт увійшли результати за такими пунктами: -аналіз сучасних криптографічних систем та методів визначення їх параметрів; -дослідження статистичних методів визначення ймовірнісних характеристик криптографічних перетворень; -створення нових ефективних методів визначення параметрів відповідних засобів КЗІ; -модифікація та створення нових способів побудови методів криптоаналізу, оцінка їх складності в класичній та постквантовій моделі обчислень; -узагальнення, оцінювання теоретичних та експериментальних результатів дослідження; пропозиції щодо можливих застосувань результатів дослідження, визначення напрямків подальших досліджень.

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: без обмежень

Закінчення етапу:

Споживачі продукції: Служба зовнішньої розвідки України

Перспективні ринки: Україна

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

IX. Бібліографічний опис

1. H.M. Heys and S.E. Tavares, Substitution-permutation networks resistant to differential and linear cryptanalysis // Journal of Cryptology, Vol. 9, No. 1, pp. 1-19, 1996.
2. J. Daemen, L. Knudsen, and V. Rijmen, The block cipher SQUARE // Fast Software Encryption (FSE'97), LNCS 1267, pp. 149-165, Springer-Verlag, 1997.
3. J. Daemen and V. Rijmen, The Design of Rijndael // AES - The Advanced Encryption Standard, Springer-Verlag, 2002.
4. S. Hong, S. Lee, J. Lim, J. Sung, and D. Cheon, Provable security against differential and linear cryptanalysis for the SPN structure // Fast Software Encryption, FSE 2000, in: Lecture Notes in Comput. Sci., Vol. 1978, Springer, Berlin, pp. 273-283.
5. J.-S. Kang, S. Hong, S. Lee, O. Yi, C. Park, and J. Lim, Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks // ETRI J. 23 (2001), pp. 158-167.
6. K. Chun, S. Kim, S. Lee, S.H. Sung, and S. Yoon, Differential and linear cryptanalysis for 2-round SPNs // Inform. Process. Lett. 87 (2003), pp. 277-282.
7. S. Park, S.H. Sung, S. Chee, E.-J. Yoon, and J. Lim, On the security of Rijndael-like structures against differential and linear cryptanalysis // Advances in Cryptology, ASIACRYPT 2002, in: Lecture Notes in Comput. Sci., Vol. 2501, Springer, Berlin, 2002, pp. 176-191.
8. S. Park, S.H. Sung, S. Lee, and J. Lim, Improving the upper bound on the maximum differential and the maximum linear hull probability for SPN structures and AES // Fast Software Encryption, FSE 2003, in: Lecture Notes in Comput. Sci., Vol. 2887, Springer, Berlin, 2003, pp. 247-260.
9. L. Keliher, H. Meijer, and S. Tavares, Improving the upper bound on the maximum average linear hull probability for Rijndael, // Eighth Annual International Workshop on Selected Areas in Cryptography (SAC 2001), LNCS 2259, pp. 112-128, Springer-Verlag, 2001.
10. L. Keliher, Refined analysis of bounds related to linear and differential cryptanalysis for the AES // Fourth Conference on the Advanced Encryption Standard, AES4, in: Lecture Notes in Comput. Sci., Vol. 3373, Springer, Berlin, 2005, pp. 42-57.
11. L. Keliher and J. Sui, Exact maximum expected differential and linear probability for 2-round Advanced Encryption Standard (AES) // Technical Report, IACR ePrint Archive (<http://eprint.iacr.org>, Paper # 2005/321), 2005.
12. Ковальчук Л.В. Обобщенные марковские шифры: построение оценки практической стойкости относительно дифференциального криптоанализа // Математика и безопасность информационных технологий. Материалы конференции в МГУ 25 - 27 октября 2006 г. - М.: МЦНМО, 2007. - С. 595 - 599.
13. Ковальчук Л.В., Шерстюк А.О., Дослідження різницевої характеристик раундової функції блочних шифрів MISTY1 та MISTY2 // Прикладна радіоелектроніка. - №3. - 2009. - С. 15-27.
14. Алексейчук А.Н., Ковальчук Л.В., Верхние границы максимальных значений вероятностей дифференциальных и линейных характеристик шифра Фейстеля, содержащего сумматор по модулю // Прикладная радиоэлектроника. - 2006. - Т. 5. - № 1. - С. 74 - 82.
15. Ковальчук Л.В., Пальченко С.В., Скрипник Л.В., Застосування теорії узагальнених марковських шифрів для оцінювання стійкості сучасних блокових алгоритмів шифрування до методів різницевого криптоаналізу // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні - К.: НДЦ "Тезіс", 2009 - №2 (19) - стор. 45-56.
16. Biham E, Shamir A., Differential cryptanalysis of DES-like cryptosystems // Journal of Cryptology. - 1991. - V. 4. - № 1. - P. 3 - 72.
17. Lai X., Massey J.L., Murphy S., Markov ciphers and differential cryptanalysis // Advances in Cryptology - EUROCRYPT'91, Proceedings. - Springer Verlag, 1991. - P. 17-38.
18. O'Connor L., Golic J.D. A unified Markov approach to differential and linear cryptanalysis // Advances in Cryptology - ASIACRYPT'94, Proceedings. - Springer Verlag, 1994. - P. 387 - 397.
19. Горбенко И.Д., Тоцький О.С., Казьміна С.В., Перспективний блоковий шифр "Калина" - основні положення та специфікація // Прикладна радіоелектроніка. - 2007. - т.6, №2. - С.195-208.
20. А. Алексейчук, Л. Ковальчук, Е. Скрынник, А. Шевцов., Оценки практической стойкости блочного шифра "Калина" относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах. // Прикладная радиоэлектроника. - №1. - 2008. - С. 203-210.
21. Kovalchuk L., Alekseyshuk A., Upper Bounds of Maximum Value of Average Differential and Linear Characteristic Probabilities of Feistel Cipher with Adder Modulo 2ⁿ, // Theory of Stochastic Processes. - 2006. - Vol. 12(28). - № 1, 2. - P. 20 - 32.
22. Ковальчук Л. Верхние оценки средних вероятностей дифференциальных аппроксимаций булевых отображений // Труды Четвёртой Общероссийской научной Конференции "Математика и безопасность информационных технологий" (МаБИТ-05), 2-3 ноября 2005. - С.163-167.
23. Ковальчук Л. Обобщенные марковские шифры: оценка практической стойкости к методу

дифференциального криптоанализа // Труды Пятой Общероссийской научной Конференции "Математика и безопасность информационных технологий" - (МаБИТ-06), 25-27 октября 2006. - С. 595-599. 24. Олексійчук А.Н., Ковальчук Л.В., Пальченко С.В. Криптографічні параметри вузлів заміни, що характеризують стійкість ГОСТ-подібних блокових шифрів відносно методів лінійного та різницевого криптоаналізу // Захист інформації. - 2007. - № 2. - С. 12 - 23. 25. Алексейчук А., Ковальчук Л., Шевцов А., Скрыпник Л. Оценки практической стойкости блочного шифра "Калина" относительно разностного, линейного билинейного методов криптоанализа. // Труды Седьмой Общероссийской научной Конференции "Математика и безопасность информационных технологий" - (МаБИТ-08), 30 октября - 2 ноября 2008. - С. 15-20. 26. А. Алексейчук, Л. Ковальчук, Е. Скрыпник, А. Шевцов. Оценки практической стойкости блочного шифра "Калина" относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах. // Прикладная радиоэлектроника. - №1. - 2008. - С. 203-210. 27. National Institute of Standards and Technology: The Advanced Encryption Standard (AES) - Режим доступа: <http://csrc.nist.gov/aes/> 28. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. - М.: Госстандарт СССР, 1989. - 28с. 29. Горбенко И.Д., Тоцький О.С., Казьміна С.В. Перспективний блоковий шифр "Калина" - основні положення та специфікація // Прикладна радіоелектроніка. - 2007. - т.6, №2. - С.195-208. 30. Горбенко И.Д., Бондаренко М.Ф. та ін. Перспективний блоковий шифр "Мухомор" - основні положення та специфікація // Прикладна радіоелектроніка. - 2007. - т.6, №2. - С.147-157. 31. X. Wang, H. Yu. How to Break MD5 and Other Hash Functions. // Advances in Cryptology EUROCRYPT'05, Lectures Notes in Computer Science 3494, Springer-Verlag, 2005, P. 19-35. 32. S. Cotini, R.L. Riverst, M.J.B. Robshaw, Y. Lisa Yin. Security of the RC6™ Block Cipher, <http://www.rsasecurity.com/rsalabs/rc6/>. 33. Tomas A.Berson Differential cryptanalysis mod with applications to MD5 // Advanced in Cryptology. - CRYPTO'98 (LNCS 372). - 1999. - P. 95-103. 34. Ковальчук Л. Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и оператора сдвига. // "Кибернетика и системный анализ" - 2010, - №6, С. 89 - 96. 35. Ковальчук Л.В., Кучинская Н.В., Скрыпник Л.В. " Построение верхних оценок средних вероятностей целочисленных дифференциалов для раундовых функций определенной структуры" // Международный конгресс по информатике: информационные системы и технологии: материалы международного конгресса, Республика Беларусь. Минск, Тезисы докладов - 2011, ст.91- 95) 36. Ковальчук Л.В., Кучинская Н. В., Скрыпник Л.В. "Определение параметров, влияющих на значение вероятности целочисленного раундового дифференциала блочного шифра" // Спеціальні телекомунікаційні системи та захист інформації. Вип. 1(21) 2012 стор. 32-43. 37. Коваленко І.М. Про алгоритм субекспоненціальної складності декодування сильно спотворених лінійних кодів // Доп. АН УРСР. Сер. А. - 1988. - № 10. - С. 16 - 17. 38. Blum A., Kalai A., Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model // J. ACM. - 2003. - Vol. 50. - № 3. - P. 506 - 519. 39. Lyubashevsky V. The parity problem in the presence of noise, decoding random linear codes, and the subset sum problem // APPROX and RANDOM'05, Proceedings. - Springer Verlag, 2005. - P. 378 - 389. 40. Kopparty S., Saraf S. Local list decoding and testing of random linear codes from high-error // <http://web.mit.edu/swastik/www/papers>. 41. Bhattacharyya A., Indyk P., Woodruff D.P., Xie N. The Complexity of linear dependence problems in vector spaces // Innovations in Computer Science - ICS 2010, Bijing, China, Jan. 7 - 9, 2011, Proceedings. - P. 496 - 508. 42. Wagner D. A generalized birthday problem // Advances in Cryptology - CRYPTO'02, Proceedings. - Springer Verlag, 2002. - P. 288 - 303. 43. Minder L., Sinclair A. The extended k-tree algorithm // The 19th Annual ACM-SIAM Symposium on Discrete Algorithms, Proceedings, 2009. - P. 586 - 595. 44. Hoeffding W. Probability inequalities for sums of bounded random variables // J. Amer. Statist. Assoc. - 1963. - Vol. 58. - № 301. - P. 13 - 30. 45. Гаврилкевич М.В., Солодовников В.И. Эффективные алгоритмы решения задач линейной алгебры над полем из двух элементов // Обзорение прикл. промышл. матем. 1995. Т. 2. Вып. 3. С. 400-437. 46. Johansson T., Jonsson F. Fast correlation attacks through reconstruction linear polynomials // Advances in Cryptology - CRYPTO'00, Proceedings. - Springer Verlag, 2000. - P. 300 - 315. 47. Fossorier M.P.C., Mihaljević M.J., Imai H., Cui Y., Matsuura K. A novel algorithm for solving the LPN problem and its application to security evaluation of the HB protocol for RFID authentication // Cryptology ePrint Archive, Report 2006/197, <http://>

// eprint.iacr.org/2006/197. 48. Балакин Г.В. Введение в теорию случайных систем уравнений // Труды по дискретной математике. М.: ТВП. 1997. Т. 1. С. 118. 49. Глухов М.М. О сложности решения систем линейных уравнений над конечным коммутативным цепным кольцом // Труды по дискретной математике. М.: ФИЗМАТЛИТ. 2002. Т. 6. С. 14-30. 50. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. - М.: Издательство иностранной литературы, 1963. - С. 333-402. 51. Ю.Н. Горчинский. О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями. // Труды по дискретной математике, М.: ТВП, 1997, т. 1, стр. 67-84. 52. Ю.Н. Горчинский. Стохастические алгебры. // Труды по дискретной математике, М.: ТВП, 1998, т. 2, стр. 55-87. 53. О.В. Шемякина. О перемешивающих свойствах операций в конечном поле. // Труды Восьмой Общероссийской научной Конференции "Математика и безопасность информационных технологий" - (МаБИТ-09), 30 октября - 2 ноября 2009, М.: МЦНМО, 2010. - Т.2 - С. 87-90. 54. Paterson K.G. Imprimitve permutation groups and trapdoors in iterated block ciphers // Fast Software Encryption. - FSE'99, Proceedings. - Springer Verlag, 1999. - P. 201-214. 55. Wagner D. Towards a unifying view of block cipher cryptanalysis // Fast Software Encryption. - FSE'04, Proceedings. - Springer Verlag, 2004. - P. 116-135. 56. О.В. Шемякина. О перемешивающих свойствах операций в конечном поле. // Труды Девятой Общероссийской научной Конференции "Математика и безопасность информационных технологий" - (МаБИТ-10), 30 октября - 2 ноября 2010, М.: МЦНМО, 2011. - Т.2 - С. 35-41. 57. Л.В. Ковальчук, О.А. Сиренко. Анализ перемешивающих свойств операций модульного и побитового сложения, определенных на одном носителе // Кибернетика и системный анализ. - 2011. - № 5. - С. 83 - 97. 58. Л.В. Ковальчук, О.А. Сиренко, Л.В. Скрыпник. Нарушение структуры факторгрупп при использовании различных групповых операций на одном носителе. // Материалы VI международной научной конференции по проблемам безопасности и противодействия терроризму. Том 2. Материалы IX общероссийской научной конференции "Математика и безопасность информационных технологий" (МаБИТ-2010), Москва, МГУ им. Ломоносова М. В., 11-12 ноября, 2010. - М., 2010. - С. 77-84. 59. Сиренко О.О. Аналіз перемішувачих властивостей операцій модульного множення та додавання в кільці. // Журнал обчислювальної та прикладної математики. - 2011. - № 1 (104). - С. 102 - 110. 11. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. // М.: Госстандарт СССР, 1989. - 28 стр. 60. И.Д. Горбенко, О.С. Тоцький, С.В. Казьміна. Перспективний блоковий шифр "Калина" - основні положення та специфікація // Прикладна радіоелектроніка. - 2007. - т.6, №2. - стр. 195-208. 61. Lai X., Massey J.L., Murphy S. Markov ciphers and differential cryptanalysis. // Advances in Cryptology - EUROCRYPT'91, Proceedings. - Springer Verlag, Berlin, 1991. - pp. 17-38. 62. Tomas A. Berson. Differential cryptanalysis mod 232 with applications to MD5 // Advanced in Cryptology. - CRYPTO'98 (LNCS 372), Proceedings. - Springer Verlag, New York Inc., 1999, - pp. 95-103. 63. Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems // Journal of Cryptology. - 1991. - V. 4. - № 1. - pp. 3-72. 64. Announcing the ADVANCED ENCRYPTION STANDART (AES). FIPS Publicattion 197, November 26, 2001. Электронный ресурс, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf> 65. Ковальчук Л.В. Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и оператора сдвига. // Кибернетика и системный анализ, №6, 2010, стр. 89-96. 66. Shamir A. How to solve it: new techniques in algebraic cryptanalysis. Crypto' 2008. 67. Dinur I., Shamir A. Cube Attacks on Tweakable Black Box Polynomials. Eurocrypt' 2009. - LNCS 5479. - Springer-Verlag. - 2009. - P. 278 -299. 68. Aumasson J-P., Dinur I., Meier W., Shamir A. Cube testers and key recovery attacks on reduced-round MD 6 and Trivium // In: Advances in Cryptology. - FSE' 2009. - LNCS 5665. - Springer-Verlag. - 2006. - P. 1 -22. 69. Dinur I., Shamir A. Side channel cube attacks on block ciphers // Cryptology ePrint Archive.- Report 2009/127. 70. Dinur I., Shamir A. Breaking Grain-128 with Dynamic Cube Attacks // Cryptology ePrint Archive.- Report 2010/570. 71. Eric Filiol. A New Statistical Testing for Symmetric Ciphers and Hash Functions. - ICICS 2002: 342-353. 72. A Statistical Test Suite For Random And Pseudorandom Number Generators For Cryptographic Applications. NIST Special Publication 800-22. 73. Nicolas T. Courtois. "About Filiol's Observations on DES, AES and Hash Functions (draft)". 74. "Handbook of Applied Cryptography", A. Menezes, P. Van Oorschot, S. Anstone, CRC Press, 1997. 75. <http://www-rocq.inria.fr/codes/Eric.Filiol/index.html>. 76. "Cryptanalysis of MD4", Hans Dobbertin, Journal of

Cryptography, 1998. 77. "NIST COMMENTS ON CRYPTANALYTIC ATTACKS ON SHA-1", <http://csrc.nist.gov/groups/ST/hash/statement.html>. 78. <http://www.oracle.com/technetwork/java/javase/downloads/index.html>. 79. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, <http://www.ipa.go.jp/security/rfc/RFC3447EN.html>. 80. <http://bouncycastle.org/>, сайт криптографічної бібліотеки. 81. Ермаков С.М., Михайлов Г.А. Курс статистического моделирования. – М.: Наука, 1976. – 319 с. 82. Шор Я.Б. Статистические методы анализа и контроля качества и надежности. – М.: Сов. Радио, 1962. – 552с. 83. Шор Я. Б., Кузьмин Ф. И. Таблицы для анализа и контроля надежности. – М.: Советское радио, 1968. 84. "Таблицы математической статистики", Большев Л.Н., Смирнов Н.В., М.: Наука, 1983. 85. H.Englund, T.Johansson, M.S.Turan. A Framework for Chosen IV Statistical Analysis of Stream Ciphers. – In: Advances in Cryptology. – INDOCRYPT' 2007. – LNCS 4859. – Springer-Verlag.-2007.-P.268-281. 86. P.Stankovski.Greedy Distinguishes and Nonrandom Detectors. – In: Advances in Cryptology. – INDOCRYPT' 2010. – LNCS 6498. – Springer-Verlag.-2010.-P.210-226. 87. M.E. Hellman, A cryptanalytic time-memory trade-off. IEEE Transactions on information theory, IT-26:401 – 406, 1980. 88. P. Oechslin, Making a faster cryptanalytic time-memory trade-off. – <http://lasecwww.epfl.ch/~oechslin/publications/crypto03.pdf> 89. E. Barkan, E. Biham, A. Shamir, Rigorous bounds on cryptanalytic time

Х. Заключні відомості

Керівник юридичної особи

Новіков Олексій Миколайович

Перелік осіб-виконавців

Єндовицький П.

Завадська Л.О.

Ковальчук Л.В.

Олексійчук А.

Фаль О.М.

Фесенко А.

Шевцов А.

Яковлев С.

**Відповідальний за підготовку
облікових документів**

Телефон

Реєстратор

**Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності**

