УДК 004.056.5

Гончар С.А., аспірант

Криптографія з часовим розкриттям: минуле, теперішнє, майбутнє

Київський національний університет імені Тараса Шевченка,03680, м. Київ, пр-т Глушкова 4д, e-mail: sg.gonchar@gmail.com

S. A. Gonchar, postgraduate

Time-release cryptography: past, present, future

Taras Shevchenko National University of Kyiv, 03680, Kyiv, Glushkova av., 4d, e-mail: sg.gonchar@gmail.com

В роботі розглянуто розвиток концепції криптографії з часовим розкриттям та запропоновано можливі шляхи розвитку цієї концепції.

Ключові слова: криптографія, часові замки, часові сервери.

The article discusses the principles of time-release cryptographic systems and its development since Rivest et al works to modern publications. There are two methods of implementing time-release cryptography: the first is based on the need to perform certain calculations in a specific period of time (time-lock puzzles), and the second requires a third party (or central authority) to carry out the process of issuing some information to open an encrypted text in a certain period or time. Method of time-lock puzzles virtually unchanged since the work of Rivest at al. However, some of its non-standard applications can be developed in a broader sense. In this paper the concept of one of these applications was designated. The use of a third party, usually a time server, received significant development after the introduction of identity base encryption since the early 2000s and reached its peak in 2008. However, new technologies have recently emerged which allow secure online transactions without relying on a central authority. Therefore, in the future such technologies should be used to create time-release cryptographic systems.

Key Words: time-release cryptography, time-lock puzzles, time server.

Статтю представив чл.-кор. НАНУ, д.ф.-м.н., проф. Анісімов А. В.

Вступ

Проблема захисту інформації шляхом її перетворення, що виключає її прочитання сторонньою особою, хвилювала людський розум з давніх-давен. У сучасній криптографії існує безліч підходів, які позволяють захищати певну інформацію. Усі ці підходи застосовуються в певних областях криптографії, які в свою чергу позволяють шифрувати та розшифровувати інформацію в реальному часі або ж з певною затримкою. Серед усіх областей досліджень в криптографії однією із найбільш цікавих і найменш досліджених є так звані "листи у майбутнє". У літературі, як правило, іноземній, для такого роду шифрування існує велика кількість термінів – "time-released crypto"[1], "timed-release encryption"[2], "timed commitments"[3], "time-lapse cryptography "[4], "time-specific encryption"[5]. У зв'язку з тим, що принципових відмінностей серед вищеназваних понять немає, то локалізована версія терміну може звучати як "криптографія з часовим розкриттям" [6]. Дана область криптографії представляє собою сукупність методів, які дозволяють зашифрувати дані таким чином, щоб забезпечити їх розшифрування після закінчення заздалегідь визначеного часу, або у заздалегідь визначений час, та виключити можливість дострокового розкриття.

На відміну від класичних методів шифрування криптографія з часовим відкриттям скоріше відповідає на питання „коли" буде розшифроване повідомлення ніж на питання „хто" його розшифрував. Дійсно, деякі практичні алгоритми, які розроблені у межах криптографії з часовим розкриттям дають можливість будь-кому відкрити зашифроване повідомлення.

Історія

Історія розвитку цієї концепції починається з роботи Мея. Проте найбільш значущою є робота Рівеста та співавторів [1], в якій вони сформулювали основні напрямки криптографії з часовим розкриттям та виділили коло її використання. Так, на думку авторів, використання підходу. що розглядається, можливо якщо [1]:

- людина, яка виступає на торгах у аукціоні бажає закрити ставку до моменту закінчення торгів;

- домовласник бажає сплатити свою заставну за допомогою зашифрованих переказів;
- хтось бажає зашифрувати свої нотатки на визначений період часу.

В подальшому сфера застосування криптографії з часовим розкриттям була розширена на ситуації, коли учасникам певного конкурсу, які знаходяться у різних частинах світу, необхідно отримати доступ до певних завдань, або існує необхідність продажу чогось у визначений час.

Підходи, запропоновані в [1], у своїй основі не змінились і до сих пір, а саме:

- використання "математичних замків з часовим механізмом" – представляють собою обчислювальні задачі, які не можуть бути вирішені без обчислення на комп'ютері протягом певного проміжку часу;
- використання третьої сторони для зберігання певної інформації, яка буде важливою в подальшому розшифровуванні повідомлення.

Розглянемо еволюцію кожного з цих підходів більш детально, та сформулюємо можливі напрямки подальшого розвитку виділеної області.

Замки з часовим механізмом

Цей підхід базується на обчислювальній складності. Пропонується використовувати певні математичні операції, які вимагають точно визначений час для їх обчислення. Розкриття таких „замків” дозволяє отримати ключ для розшифрування самого повідомлення.

На етапі розробки основних принципів цього методу виділяли наступні його недоліки:

1. Проблема синхронізації часу для обчислення та реального часу – відсутня можливість відкриття ключа у точно визначений період часу, що пов’язано з різними швидкостями роботи різних комп’ютерних систем.

2. Таке шифрування є практично неможливим у випадку необхідності зберігання даних довготривалий період часу (декілька років). Це пов’язано з тим, що даний підхід потребує безперервних обчислювань, що, у свою чергу, унеможливлює використання для таких цілей персональні комп’ютери.

3. Використання даного підходу унеможливлює обчислення замків шляхом використання паралельного обчислення.

Якщо перші два недоліки актуальні і на сьогоднішній день, то метод усунення останнього був запропонований ще Рівестом та співавторами у [1]. Він, майже не змінившись, використовується і тепер та базується на повторному піднесенні у квадрат.

Так, якщо необхідно передати повідомлення M, яке зашифроване на час T, відправник має зробити наступні кроки:

- Генерується складена величина $n = pq$, в якій p и q – два випадково обраних великих числа.
- Обраховується $\phi(n) = (p-1)(q-1)$.
- Обраховується $t = TS$, де S – число піднесень у квадрат за модулем n у секунду, що може забезпечити техніка одержувача.
- Генерується випадковий ключ K для загально прийнятої криптосистеми (наприклад $RC5$). Довжина ключа повинна бути такою, щоб його підбір був недоцільним у порівнянні з часом обчислення замка.
- Ключем K зашифровується повідомлення M, таким чином отримуємо зашифрований текст $C_M = RC5(K, M)$.
- Випадковим чином обирається a по модулю n ($1 < a < n$) та зашифровується K методом обчислення $C_K = K + a^{2^t} (\mathrm{mod}\, n)$. Для більшої ефективності спочатку обчислюється $e = 2^t (\mathrm{mod}\, \phi(n))$, а потім $b = a^e (\mathrm{mod}\, n)$.
- В результаті получаємо замок (n, a, t, C_K, C_M) та видаляємо усі змінні, що залишилися (наприклад p, q) від попередніх розрахунків.

Для розшифрування ключа не залишається нічого іншого як отримати b шляхом послідовного піднесення у квадрат t раз. При цьому процес обчислення не може проводитися паралельно та залежить тільки від потужності даного комп’ютеру. Рівест запропонував варіант реалізації замка, що представляє собою, за визначенням авторів, „часову капсулу”, яка присвячена річниці лабораторії, у якій вони працювали. Цікаво, що обчислення цієї „капсули” на момент створення було розраховане на декілька років.

Подальший розвиток даного підходу пов’язаний з розширенням математичної основи для реалізації криптографії з часовим розкриттям з використанням замків. Зокрема такі питання розглядаються в [7].

Єдиною спробою модернізації існуючого підходу можна вважати підхід, викладений у [8]. Автори статті дослідили можливість створення часових замків у моделі випадкового оракула,

який представляє собою ідеалізовану функцію, що описує роботу машини з практично нескінченним об'ємом пам'яті, яка на будь-який запит може видати ідеальне випадкове число і запам'ятати пару «запит-відповідь». Основний результат роботи – негативний: виключається можливість створення часових замків, які потребують більшого часу для обчислення, ніж загальна робота, необхідна для генерації замка. Зокрема, викреслюється генерація конструкцій на зразок чорної скриньки, які базуються на часових замках, за допомогою односпрямованих перестановок та хеш-функцій. З іншого боку був сконструйований часовий замок за допомогою одного циклу n паралельних запитів до випадкового оракула, при тому, що для його обчислення потрібно n циклів послідовних запитів.

Варто, втім, відзначити один нестандартний підхід, який в подальшому може мати перспективу розвитку в більш загальному напрямку. Так, Ебрінджер в своїй статті [9] використовував задачі з часовим замком для введення в оману антивірусних аналізаторів щодо безпеки досліджуваного об'єкта. Зокрема в виконуваному файлі, який несе в собі шкідливу програму, створюється, так звана "анти-емуляторна" оболонка, яка захищає упаковку шкідливої програми від емулятора антивірусної програми. Саме ця оболонка і являє собою "замок".

Автор не ставив своїм завданням будь-яким чином модернізувати існуючі шкідливі програми, а хотів показати працездатність свого припущення і продумати можливий захист від такої схеми.

Як результати цієї роботи, так і результати заснованої на ній роботи [6] показують, що при використанні досить великих ступенів при піднесені числа за модулем шкідливий код не розпізнається.

Таке, досить вузьке використання "замків" можна розширити наступним чином: у виконуваний файл записується повідомлення (зашифроване), ключ, інформація про дату або час його розпакування, а також модуль, який опитує який-небудь або кілька публічних часових серверів і саморозпаковується в необхідний час. Дослідження можливості використання такої схеми представлення виходить за рамки цієї статті і буде розглянуте у подальшому.

Делегування повноважень третій стороні

Цей підхід спочатку був сформульований Меєм. Проте в його протоколі не гарантувалася анонімність: сервер знав повідомлення, час розкриття та учасників, які брали участь у груповій сесії(відправник та одержувач). Рівест та співавтори змінили цей протокол так, що серверу необхідно було видавати лише серію ітерацій результатів односторонньої функції ключа. Таким чином оригінальне повідомлення не зберігалось не сервері.

Коротко цей протокол можна сформулювати наступним чином: третя сторона не зберігає у себе повідомлення, а лише виконує шифрування повідомлення або частини повідомлення y ключем s_{it}, де i – певна третя сторона, яка публікує ключ s_{it} через деякий час t. Тобто отримавши запит виду „ось значення y та t, поверніть, будь ласка, $E(s_{it}, y)$, що зашифроване ключем s_{it}, який ви розкриєте у момент часу t”, третя сторона повертає зашифроване відкритим ключем відправника та підписане третьою стороною повідомлення $\left(i, t, t_0, E(s_{it}, y)\right)$

До появи шифрування на основі особистих даних (identity based encryption) здійснювалися лише спроби розвинути оригінальну ідею Рівеста та співавторів. Зокрема, було безліч спроб мінімізувати взаємодію користувача і сервера, гарантувати розширюваність і анонімність користувача. Розглянемо основні публікації за цим напрямом.

Так в роботі [10] була поставлена наступна задача: як може відправник, без постійного опитування сервера, створити документ з часом розкриття так, що одержувач зможе розшифрувати його тільки після часу розкриття, і так, що серверу не буде відома особистість відправника. Своє завдання автори вирішують на основі модифікації "забудькуватої" передачі даних (oblivious transfer data). При цьому відправник контактує безпосередньо з одержувачем, а той вже у свою чергу контактує з "часовим" сервером. При цьому сервер відповідає тільки за відповіді на запити про час від одержувача. Питання про те, яка інформація буде відправлена одержувачу після часу розкриття, автори пропонують вирішити наступним чином: відправник шифрує повідомлення спочатку відкритим ключем одержувача, а потім відкритим ключем сервера. При цьому після часу розкриття сервер на запит одержувача відправляє йому розшифроване повідомлення.

Боне і Нао в роботі [11] створили криптографічний примітив з часовим розкриттям, який вони назвали "тимчасові зобов'язання" (time commitments). Серед іншого вона могла застосовуватися для вирішення проблеми чесності цифрового підпису на контрактах.

В [4] автори дали назву, розробили і детально виклали концепцію так званої "криптографії з розривом у часі" (time-lapse cryptography), за допомогою якої повідомлення відправника обов'язково буде розкрито в певний момент часу, навіть якщо це небажано для відправника. В основу розробки лягли схема створення розподілених ключів Педерсена, пороговий розподіл секрету Фелдмана і Ель-Гамаль шифрування, кожна з яких базується на схемі Діффі-Хеллмана. Автори розглянули можливі атаки і способи захисту від них, а також описали важливі застосування свого сервісу в закритих ставках на аукціонах, біржових продажах, клінічних випробуваннях та електронному голосуванні. За словами авторів, їх концепція схожа на концепцію запропоновану Рівестом і співавторами, але замість однієї третьої сторони використовується мережа третіх сторін.

Докладно і досить просто основні поняття сучасної криптографії з часовим розкриттям, які використовують третю сторону (як правило сервер) розглянуті в презентації [12].

На рис. 1 приведена схема, яка показує еволюцію основних протоколів.

Автори цієї презентації в іншій своїй роботі [7] розглянули питання математичної основи необхідної для реалізації криптографії з часовим розкриттям, включаючи квадратичні залишки і питання білінійних схем Діффі-Хеллмана, навівши приклади для кожного з розглянутих підходів.

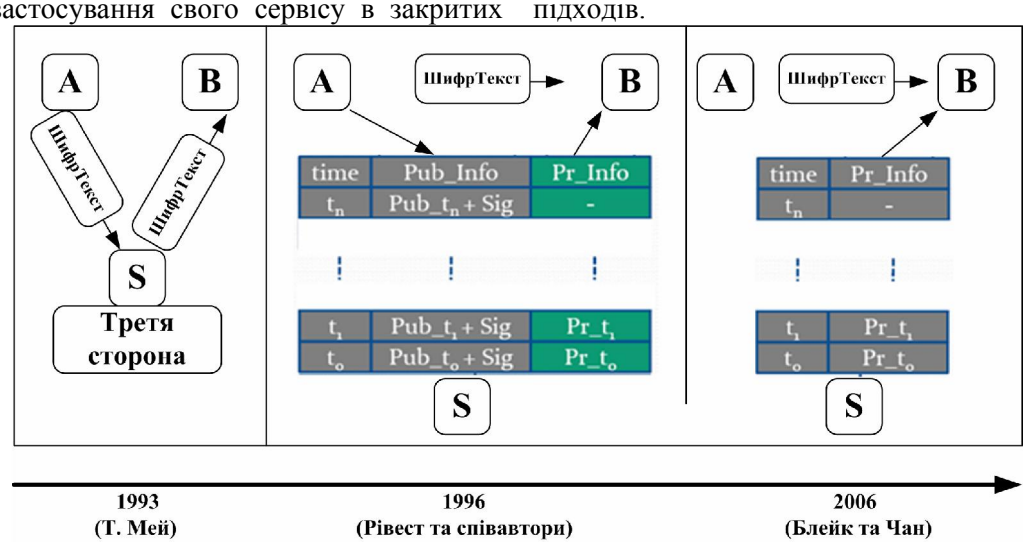

Рис. 1. Схеми шифрування з часовим розкриттям різних авторів

Прорив в питаннях криптографії з часовим розкриттям відбувся після введення шифрування на основі особистих даних. Основою такого типу шифрування є те, що відправник шифрує повідомлення M під особистість конкретного одержувача. Формально таке шифрування можна визначити як кортеж з чотирьох рандомізованих алгоритмів [13]:

- Встановлення (1^k). При вході на цей алгоритм параметра безпеки 1^k , генеруються відкриті параметри π_{IBE}, що містять у собі хеш-функції та повідомлення M . Додатково генерується основний секрет δ_{IBE} , який залишається конфіденційним завдяки серверу.
- Отримання $(\pi_{IBE}, \delta_{IBE}, I)$. Маючи на вході відкриті параметри π_{IBE}, основний секрет δ_{IBE} та характеристики особистості I , видають на вихід закритий ключ sk_I .
- Шифрування (π_{IBE}, I, M) . Генерує шифротекст c на основі вхідних параметрів π_{IBE}, I, M .
- Дешифрування $(\pi_{IBE}, sk_I, \hat{c})$. Видає на вихід оригінальне повідомлення відповідно до $\hat{c}$, або повідомлення про помилку.

Починаючи з 2003 року були запропоновані різні протоколи, які базуються на квадратичних залишках і на властивостях білінійного спарювання (відображення) в групах еліптичних кривих.

На сьогоднішній день існує досить багато напрацювань з використанням шифрування на

основі особистих даних, тому розглянемо лише основні з них.

В роботі [14] автори відштовхувалися від схеми запропонованої Блайк і Чан, в якій сервер не взаємодіє з відправником та одержувачем. Це досягається за допомогою періодичної генерації специфічних часових "лазівок", які дозволяють виконувати дешифровку тексту зашифрованого "на майбутнє" або "лазівок" для цифрового підпису. Дана концепція отримала назву шифрування з часовим розкриттям без взаємодії. Запропонована схема використовує групи білінійних відображень і припускає, що зашифрований текст завжди містить інформацію про час розкриття, яка приводитися в кінці повідомлення. Крім цього, схема запропонована авторами може бути використана при необхідності розкриття тексту в разі настання певної події.

Дуже докладно питання створення криптосистеми з часовим розкриттям за допомогою шифрування на основі особистих даних розглянуто в роботі [5]. Свій метод автори назвали „шифрування визначене у часі" (time-specific encryption).

Згідно цього методу часовий сервер розсилає так званий „постійний у часі" ключ на початку кожного часового інтервалу. Цей ключ доступний для всіх користувачів та вміщує у собі характеристику часу t . Відправник може визначити будь-який інтервал часу під час процесу шифрування, а одержувач може відновити оригінальне повідомлення тільки якщо має „постійний у часі" ключ, який відповідає часу у заданому відправником інтервалі. При цьому одержувачі додатково забезпечуються закритими ключами та або відкритими ключами або параметрами на основі особистих даних, а дешифрування потребує використання як закритого ключа так і відповідного „постійного у часі" ключа. Це забезпечує захист проти нечесного часового серверу, та можливість дешифровки тексту лише для обраної групи користувачів. Автори у [5] особливу увагу приділили безпеці розроблених схем, наголошуючи, що найбільш ефективні конструкції можуть бути отримані лише при використанні моделі випадкового оракулу.

Зазначимо, що всі сучасні схеми криптографії з часовим розкриттям (наприклад [13]), які базуються на білінійному спарюванні, вимагають наявності абелевої адитивної скінченої групи G_1 першого порядку q, і абелевої мультиплікативної циклічної групи того ж порядку G_2. Абелева група це пара $G = (A, *)$, де A – це певна множина, а $*$ - це бінарна операція на A, тобто будь-яким двом елементам a та b з A ставиться у відповідність елемент $a * b$, що також належить A.

Зокрема цей математичний апарат використовується для створення білінійного генератора параметрів Діффі-Хеллмана, що являє собою алгоритм, який при поданні на його вхід додатного цілого числа видає на вихід q.

Висновки

Незважаючи на певні обмеження щодо практичного застосування, криптографічні системи з тимчасовим розкриттям займають цілком певну нішу в галузі безпечної передачі повідомлень. Зокрема це можуть бути електронні аукціони, депонування ключів, виплати за розкладом, закриті ставки на аукціонах, лотереї і т.д.

Очевидно, що кожен з напрямків має свої шляхи розвитку.

Так, у сенсі вирішення проблеми завантаження комп'ютера при обчисленні задач з замком, перспективними є використання багатопроцесорних систем.

Викладена вище концепція використання криптографії з тимчасовим розкриттям з "замком" для створення оболонки в виконуваному файлі з повідомленням, який повинен опитувати деякий часовий сервер і самостійно розшифровувати закладене в ньому повідомлення також має місце для існування.

Для криптографії з тимчасовим розкриттям на основі серверів за останні роки створено безліч як практичних, так і теоретичних напрацювань. Однак розвиток криптографічного інструментарію дасть певний розвиток і цьому напрямку. Очевидно, що можливим і бажаним напрямком такого розвитку може бути створення систем, які не використовують сервери як такі. Зокрема, перспективним може бути використання "bitcoin"-схем.

До того ж певний інтерес має проблема приховання часу відкриття у схемах з використанням серверу від злочинців.

Список використаних джерел

1. Rivest R. L. Time-lock puzzles and timed-released crypto / R. L. Rivest, A. Shamir,

References

1. RIVEST R. L., SHAMIR A. and WAGNER D. A. (1996) *Time-lock puzzles and timed-released*

D. A. Wagner // Massachusetts Institute of Technology. – Cambridge, MA, USA. – 1996. – 9 p.

2. Crescenzo G. Conditional oblivious transfer and timed-release encryption / G. Crescenzo, R. Ostrovsky, S. Rajagopalan // Lecture notes in computer science.– 1999.– volume 1592.– P. 74 – 89.

3. Boneh D. Timed commitments / D. Boneh, M. Naor // Lecture Notes in Computer Science. – 2000. – volume 1880. – P. 236 – 254.

4. Rabin M. O. Time-Lapse Cryptography. Technical Report TR-22-06 / M. O. Rabin, C. Thorpe // Harvard University, School of Engineering and Applied Science, 2006. – 16 P.

5. Paterson K. G. Time-specific encryption / K. G. Paterson , E. A. Quaglia // Lecture notes in computer science. – 2010. – vol. 6280. – P. 1 – 16.

6. Усенко А. В. Использование криптографии с временным раскрытием для противодействия проактивным технологиям детектирования вредоносных программ / А. В. Усенко // Молодой ученый. – 2012. – №2. – С. 66 – 70.

7. Chalkias K. Mathematical problems and algorithms for timed-release encryption / K. Chalkias, F. Baldimtsi, D. Hristu-Varsakelis, G. Stephanides // Bulletin of the Transilvania University of Brasov. – 2008. – vol. 15(50). – 10 P.

8. Mahmoody M. Time-lock puzzles in the random oracle model / M. Mahmoody, T. Moran, S. Vadhan // Lecture notes in computer science. – 2011. – vol. 6841. – P 39-50.

9. Ebringer T. Anti-emulation through time-lock puzzles / T. Ebringer // Second International CARO Workshop. – Hoofddorp, Netherlands, 2008. – 10 p.

10. Crescenzo G. Conditional oblivious transfer and timed-release encryption / G. Crescenzo, R. Ostrovsky, S. Rajagopalan // Lecture notes in computer science. – 1999. – volume 1592. – P. 74 – 89.

11. Boneh D. Timed Commitments / D. Boneh, M. Naor // Lecture Notes in Computer Science. – 2000. – volume 1880. – P. 236 – 254.

12. Chalkias K. Pairing based timed-release cryptography / K. Chalkias, F. Baldimtsi, D. Hristu-Varsakelis, G. Stephanides // Identity Based Encryption Workshop. – Thessaloniki, Greece, 2008. – P. 1-65.

13. Cathalo J. Efficient and non-interactive timed-release encryption / J. Cathalo, B. Libert, J. Quisquater // Lecture Notes in Computer Science. – 2005. – volume 3783. – p. 291 – 303.

14. Cheon J. H. Provably secure timed-release public key encryption / J. H. Cheon, N. Hopper, Y. Kim, I. Osipkov // ACM Trans. Inf. Syst. Secur. – 2008. – vol. 11. – 44 P.

crypto Cambridge, MA, USA.

2. CRESCENZO G., OSTROVSKY R. and RAJAGOPALAN S. (1999) *Conditional oblivious transfer and timed-release encryption*. Lecture notes in computer science. 1592. p.74-89.

3. BONEH D. and NAOR M. (2000) *Timed commitments*. Lecture Notes in Computer Science. 1880. p.236-254.

4. RABIN M. O. and THORPE C. (2006) *Time-Lapse Cryptography. Technical Report TR-22-06*. Harvard University Press.

5. PATERSON K. G. & QUAGLIA E. A. (2010) *Time-specific encryption*. Lecture notes in computer science. 6280. p.1-16.

6. USENKO A.V. (2012) *Using time-release cryptography to counteract proactive technologies for malware detection*. Young scientist. 2. p.66-70.

7. CHALKIAS K. et al (2008) *Mathematical problems and algorithms for timed-release encryption*. Bulletin of the Transilvania University of Brasov. 15(50). p.1-10.

8. MAHMOODY M., MORAN T. and VADHAN S. (2011) *Time-lock puzzles in the random oracle model*. Lecture notes in computer science. 6841. p.39-50.

9. EBRINGER T. (2008) *Anti-emulation through time-lock puzzles*. Hoofddorp, Netherlands.

10. CRESCENZO G. , OSTROVSKY R. and RAJAGOPALAN S. (1999) *Conditional oblivious transfer and timed-release encryption*. Lecture notes in computer science. 1592. p.74-89.

11. BONEH D. and NAOR M. (2000) *Timed Commitments*. Lecture Notes in Computer Science. 1880. p.236-254.

12. CHALKIAS K. et al (2008) *Pairing based timed-release cryptography*. Identity Based Encryption Workshop. Thessaloniki, Greece. p.1-65.

13. CATHALO J., LIBERT B. and QUISQUATER J. (2005) *Efficient and non-interactive timed-release encryption*. Lecture Notes in Computer Science. 3783. p.291-303.

14. CHEON J. H. et al (2008) *Provably secure timed-release public key encryption*. ACM Trans. Inf. Syst. Secur. 11. p.1-44.

Надійшла до редколегії 23.10.14