© Kovalenko B. Development of SETUP-free cryptographic protocols // Ukrainian Scientific Journal of Information Security, 2019, vol. 25, issue 2, pp. 88-95.

DOI: 10.18372/2225-5036.25.13840

ПОБУДОВА КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ ВІЛЬНИХ ВІД КЛЕПТОГРАФІЧНИХ МОДИФІКАЦІЙ

Богдан Коваленко

ТОВ «Глобаллоджик Україна»

КОВАЛЕНКО Богдан Анатолійович

Рік і місце народження: 1990, м. Кам'янець-Подільський, Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут ім. І. І. Сікорського», 2013 рік.
Посада: інженер інформаційної безпеки.
Наукові інтереси: криптологія, клептографія, безпека технології блокчейн.
Публікації: більше 10 наукових праць, серед яких наукові статті, матеріали та тези доповідей на конференціях та семінарах, патент.
E-mail: animantbk@gmail.com.
Orcid ID: 0000-0001-7802-0587.

Анотація. *З широким розповсюдженням гібридних криптосистем у інформаційно телекомунікаційних системах, особливої гостроти набувають задачі захисту даних криптосистем на всіх рівнях життєвого циклу. Однією з характеристик сучасних криптосистем є розповсюдження їх використання в тому числі і в слабко захищених пристроях, що породжує нові вектори атак, зокрема клептографічних атак, наприклад, з модифікацією реалізації криптосистеми на кінцевому пристрої. Такі типи атак є особливо небезпечними, враховуючи той факт, що жертва зловмисника, будучи частиною певної захищеної системи (електронного документообігу, платіжної системи, секретного зв'язку тощо), може нести загрозу також для не скомпрометованих учасників системи (наприклад, витік спільних секретних даних). Одним з напрямків вирішення цієї проблеми є побудова криптосистем, стійких до різних типів клептографічних атак. З огляду на це, в статті викладено результати щодо побудови криптографічних протоколів, що стійкі до атак клептографічної модифікації реалізації. Спершу, будується формальна модель протоколу типу ''запит-відповідь'' (''challenge-response'') з клептографічним каналом витоку секрету (subliminal channel). На основі запропонованої моделі визначаються достатні умови, за яких канал непомітного витоку не може бути побудованим, формулюється та доводиться теорема про достатні умови відсутності клептографічного каналу витоку. Також в статті пропонуються модифікації двох базових протоколів -- генерації попсе та 1-прохідний протокол узгодження спільного ключа Діффі-Хеллмана, що побудовані з урахуванням достатніх умов. На основі формалізації запропонованих модифікацій було сформульовано та доведено теореми про відсутність клептографічних каналів витоку у даних протоколах. Наведені результати можуть бути використаними для побудови інших протоколів з доведеною відсутністю прихованих каналів витоку, що допомагає вирішити одну з практичних клептографічних задач для підвищення загальної безпеки криптосистеми.*

Ключові слова: *клептографія, SETUP, канали непомітного витоку секрету, протокол Діффі-Хеллмана, гібридна криптосистема, subliminal channel, challenge-response protocol.*

Актуальність проблеми дослідження

У сучасних гібридних системах зв'язку одним із важливих напрямів криптологічних досліджень є дослідження клептографічних можливостей, тобто оцінка та зменшення ризиків, пов'язаних з можливістю впровадження до систем лазівок, що ведуть до порушення деяких з властивостей інформації для розробника, що знає секрет лазівки. Ймовірність таких сценаріїв підвищує той факт, що більшість практичних реалізацій криптосистем функціонує у незахищеному середовищі.

Загалом, за рівнем побудови, можна виділити два класи клептографічних механізмів: ті, що вбудовуються на етапі проектування криптосистеми і такі, що будуються шляхом модифікації існуючої криптосистеми чи протоколу. Механізми другого типу, а саме, схеми типу SETUP (Secretly Embedded Trapdoor with Universal Protection) були запропоновані А. Яном та М. Юном [3]. Принцип роботи такої схеми полягає в тому, що в протокол взаємодії абонентів додається додаткова роль – розробник, що модифікує реалізацію протоколу одного з абонентів (шляхом несанкціонованого доступу до ресурсів абонента чи розповсюдження зловмисного програмного забезпечення) таким чином, що жертва починає передавати певний секрет розробнику, при чому інші абоненти за здатні цього виявити.

Актуальність даних досліджень випливає з актуальності аналізу стійкості криптографічних протоколів, в т.ч. задач виявлення нових векторів атак на існуючі комплексні системи захисту інформації. Криптографічні протоколи є важливим компонентом будь якої системи віддаленого доступу (фронтенд), в той час як для деяких технологій (наприклад, блокчейн технологій розподіленого реєстру) є базовим функціональним компонентом системи.

Задачами клептографії в контексті криптографічних протоколів є:

1. Побудова лазівок у стандартних протоколах.
2. Виявлення лазівок.
3. Побудова криптографічних протоколів із доведеною відсутністю лазівок.

Наразі, відомі численні приклади теоретичних та практичних схем побудови каналів непомітного витоку секрету в криптографічних схемах. В даній роботі основна увага приділяється вирішенню проблеми визначення умов за яких побудова лазівки практично не можлива, тобто схем з доведеною відсутністю каналів непомітного витоку секрету.

Сучасний стан досліджень механізмів SETUP

Одним з методів клептографічних механізмів на основі криптосистем є SETUP [1] (Secretly Embedded Trapdoor with Universal Protection – таємно вбудований захищений канал витоку секрету). Ідея роботи SETUP полягає у тому, що зловмисник модифікує реалізацію стандартної криптосистеми таким чином, що для розробника не виконуються криптографічні властивості системи, а для інших користувачів вона залишається такою ж стійкою. Більш того, інші учасники не можуть навіть запідозрити факт такої модифікації. Окрім власне SETUP також розрізняють слабкий та сильний SETUP.

SETUP криптосистеми C називають таку її модифікацію C′, що:

1. Інтерфейс взаємодії (вхідні та вихідні параметри) з C′ відповідає заявленому для C стандарту.
2. C′ ефективно обчислюється.
3. Секрет розробника наявний лише у нього і не міститься в C′.
4. Секретна інформація, яку C′ надсилає до каналу витоку, може бути ефективно розшифрована лише розробником (розробник використовує свій секретний ключ для розшифрування).
5. Ніхто, окрім розробника, не може розрізнити за поліноміальний час виходи систем C′ та C.
6. Після аналізу модифікованої реалізації (отримання всіх необхідних алгоритмів, деструктивний реверс інжиніринг) неможливо відновити попередні або спрогнозувати майбутні ключі.

Слабким SETUP називається SETUP для якого розрізнити виходи C та C′ може не лише розробник, а і власник модифікованої реалізації

Сильним SETUP називається SETUP з додатковою умовою – неможливо відновити попе-редні та спрогнозувати наступні ключі не лише після деструктивного аналізу, але і у випадку аналізу стану системи в режимі реального часу.

Важливою характеристикою SETUP механізму є ширина пропускання (bandwidth). (n,m)-схемою витоку секрету називається SETUP механізм, якому необхідно передати m повідомлень захищеним каналом для здійснення витоку n повідомлень.

Наразі всі відомі SETUP механізми побудовані на базі асиметричних криптопримітивів для багатьох криптосистем: систем цифрового підпису ([1]), системах, що базуються на проблемах дискретного логарифму ([4]) та RSA ([3]).

SETUP на основі задачі дискретного логарифмування

Ідея схеми авторів SETUP полягає у тому, що сторона, яка генерує пари ключів та публікує публічні, має модифіковану реалізацію, що передає захищеним каналом розробнику секретні ключі.

Генерація сеансових публічних ключів з прихованим витоком секретного ключі.

Вихідні дані:

1. F_p^* – мультиплікативна група з генератором g.
2. $(x, Y = g^x \mathrm{mod} p), x, Y \in F_p^*$ – пара ключів розробника.
3. $W, a, b \in F_p^*$ – фіксовані параметри.

Кроки роботи алгоритму генерації публічних сеансових ключів:

1. Генерується випадковий ключ $c_1 \in F_p^*$. c_1 зберігається для генерації наступного ключа.
2. Обчислюється та публікується перший публічний ключ $\underline{M_1 = g^{c_1} \mathrm{mod} p}$.
3. Генерується випадкове $t \in \{0,1\}$.
4. Обчислюється $z = g^{c_1 - Wt} Y^{-ac_1 - b} \mathrm{mod} p$.
5. Обчислюється наступний секретний ключ: $c_2 = hash(z), hash: \{0,1\}^* \to F_p^*$.
6. Обчислюється та публікується відкритий ключ $\underline{M_2 = g^{c_2} \mathrm{mod} p}$.

Кроки роботи алгоритму відновлення другого сеансового секретного ключа розробником:

1. $r = M_1^a g^b \mathrm{mod} p$.
2. $z_1 = M_1 / r^x \mathrm{mod} p$.
3. $c_2 = hash(z_1)$ або $c_2 = hash(z_1 / g^W \mathrm{mod} p)$.

Таким чином, розробник може отримати секретний ключ c_2 і ніхто не зможе його отримати без знання секретного ключа розробника x.

Викладення основного матеріалу

Для оцінки стійкості клептографічної системи перш за все необхідно визначитися з моделлю складності. В криптографії виділяють декілька основних моделей: теоретико-обчислювальна, теоретико-інформаційна, зведення до практичних конструкцій. Ці моделі не завжди повністю відображатимуть картину стійкості клептографічного механізму. Наприклад, якщо ми складність побудови лазівки симетричного шифру є екпоненційним відносно розміру внутрішнього стану, але тим не менш побудувати лазівку можливо за практичний час, то такий метод побудови лазівки має право на життя. З іншого боку, якщо асимптотична складність виявлення лазівки є поліномом високої степені від розміру внутрішнього стану, але для заданої параметрів криптосистеми цей час є непрактичним, то можна говорити про стійкість лазівки до виявлення в практичному сенсі.

У роботі [2] використовується модель, що базується на практичній складності виконання алгоритму.

У даній роботі пропонується використовувати схожу модель складності, що базується на практичній складності обчислення.

Визначення 1 *(практичний класифікатор ансамблів). Нехай існує два ансамблі* $E = \{e_1, e_2, \dots\}$ *та* $E' = \{e'_1, e'_2, \dots\}$, $e_i, e'_i \in S$. *Додатково заданий часовий поріг* t, *максимальний час, що відпускається на виконання алгоритму (наприклад,* $t = 2^{80}$*).*

Класифікатором ансамблів називатимемо ймовірнісний розпізнавальний алгоритм A_t, обмежений часом роботи t, що для вектору довжини l, $\vec{v} \in E^l \cup E'^l$, повертає значення:

$$\begin{cases} A_t(E, v) = 1 & \Leftrightarrow v \in E^l \\ A_t(E', v) = 1 & \Leftrightarrow v \in E'^l. \end{cases}$$

Також визначимо перевагу (advantage) практичного класифікатора у розпізнаванні ансамблів як

$$Adv_{A_t}(E, E', l) = |P\{A_t(E, \vec{v}) = 1\} - P\{A_t(E', \vec{v}) = 1\}|,$$

де $\vec{v} \in E^l \cup E'^l$ – випадковий вектор довжини l.

Визначення 2 *(практична нерозрізненість). Два ансамблі* E *та* E' *називаються практично нерозрізнені (practical indistinguishable) для заданого параметру безпеки* t, *якщо максимальна перевага у розпізнаванні для всіх практичних алгоритмів буде незначною відносно параметра безпеки:*

$$Adv(E, E') = max_{l, A_t}\{Adv_{A_t}(E, E', l)\} < \varepsilon(t),$$

де $\varepsilon(t)$ *– порогове значення для "незначної" ймовірності (наприклад,* $\varepsilon(t) = 2^{-40}$ *при* $t = 2^{80}$*).*

Надалі, для практично нерозрізнених множин E та E' використовуватимемо позначення $E \simeq_t E'$.

Визначення SETUP, що було запропоноване Яном і Юном [3] є не занадто формалізованим, що ускладнює оцінки складності побудови та пошуку. Однією з базових криптосистем є протоколи типу "запит-відповідь", за допомогою яких можна описати практично будь-який одно та двопрохідний протоколи, наприклад, схеми аутентифікації на основі симетричного шифру, узгодження ключа Діффі-Хеллмана тощо. Також, на основі протоколу типу "запит-відповідь" побудуємо модель клептографічного механізму для немопітного витоку секрету, що є важливим частковим випадком схеми SETUP.

Протокол типу "запит-відповідь" моделюється грою з $N > 1$ учасниками, один з яких є оракулом.

Клептографічний варіант протоколу також включає ще одного учасника – розробника, що з яким один з учасників знаходиться у змові.

Визначення 3 *(клептографічний механізм на базі протоколу "запит-відповідь"). Клептографічним варіантом базового протоколу типу "запит-відповідь" називатимемо гру між 3-ма учасниками (Alice, Bob та Dev) з такими правилами:*

1. Сторони Alice та Dev можуть бути змовниками.

2. Сторона Alice очікує на запит сторони Bob, після якого вона має повернути відповідь у форматі, що заздалегідь узгоджений з Bob. Задачами Alice є:

(a) сформувати відповідь, що кодує один біт інформації, яку сторона Dev може ефективно відновити;

(b) кодування має відбуватися таким чином, щоб сторона Bob не могла розпізнати факту передачі.

3. Сторона Bob посилає довільний запит стороні A і отримує відповідь. Задачею Bob є виявлення факту передачі додаткової інформації стороні Dev.

4. Сторона Dev пасивно прослуховує трафік між Alice та Bob. Задачею сторони Dev є відновлення біту інформації від сторони Alice на основі перехоплених повідомлень.

Також вважатимемо дійсними такі припущення:

1. Сторона Bob не змовляється ні з Alice ні з Dev.

2. Усі сторони використовують стандартні базові криптопримітиви та не містять закладок.

3. Alice та Dev не використовують додаткові стеганографічні канали, що базуються на часових затримках протоколу, збоях у роботі тощо.

З точки зору сторони Bob, яка має виявляти факт витоку секрету, протокол може бути представленим у вигляді кортежу $\langle D, V, U \rangle$, де V – множина запитів сторони Bob, U – множина відповідей оракула Alice, $D_t: V \times U \to \{0,1\}$ – ймовірнісний алгоритм, обмежений часом роботи t, що перевіряє відповідь оракула на відповідність протоколу.

З боку розробника Dev, до кортежу також додається $R_t^\omega: V \times U \to \{0,1\}$ – алгоритм, що обчислює повідомлення, передане стороною Alice.

Визначення 4 *(протокол "запит-відповідь", формальна модель). Протоколом типу "запит-відповідь" називатимемо кортеж* $\langle D_t, V, U, A_t \rangle$, *де:*

– $D_t: V \times U \to \{0,1\}$ – ймовірнісний алгоритм, обмежений часом роботи t, що перевіряє відповідь оракула на відповідність протоколу. Кожну коректну пару запит-відповідь алгоритм розпізнає з ймовірністю 1, тобто є алгоритмом типу Монте-Карло.

– V – множина запитів сторони Bob, U – множина відповідей оракула Alice.

– $A_t: V \to U$ – рандомізований алгоритм оракула Alice без витоку секрету: $\forall v \in V: D_t(A_t(v)) = 1$.

Визначення 5 *(канал витоку на базі протоколу "запит-відповідь", формальна модель). Протоколом типу "запит-відповідь" з каналом витоку називатимемо кортеж з моделі 4* $\langle D_t, V, U, A_t, R_t^\omega, A_t^\omega \rangle$ *з додатковими параметрами* R_t^ω *та* A_t^ω *(канал витоку), де* D_t, V, U, A_t *мають той же сенс, що і в моделі 4:*

$A_t^\omega: V \times \{0,1\} \to U$ – рандомізований алгоритм оракула Alice з витоком секрету:

$$\forall v \in V, s \in \{0,1\}: D_t(A_t^\omega(v, s)) = 1, v \overset{rand}{\in} V, s \in \{0,1\}: P\{R_t^\omega(v, A_t^\omega(v, s)) = s\} > 1/2 + \varepsilon(t).$$

$R_t^\omega: V \times U \to \{0,1\}$ – ймовірнісний алгоритм, що декодує повідомлення, передане стороною Alice, на основі секрету ω.

Додатково накладаються умови секретності та непомітності каналу: множини

$$H = \{\langle v, u \rangle | v \in V, u \in U: u = A_t(v)\}, H_0 = \{\langle v, u \rangle | v \in V, u \in U: u = A_t^\omega(v, 1)\} \text{ та } H_1 = \{\langle v, u \rangle | v \in V, u \in U: u = A_t^\omega(v, 0)\}$$

є попарно практично нерозрізненими: $H \simeq_t H_0 \simeq_t H_1$.

Також додається припущення про відсутність інформації для розробника з виходу алгоритму A_t: $|P\{R_t^\omega(v, A_t(v)) = 0\} - P\{R_t^\omega(v, A_t(v)) = 1\}| < \varepsilon(t)$.

Визначення 6 *(рівність рандомізованих алгоритмів). Рандомізовані алгоритми* $A_t, A'_t: \mathfrak{Q}_1 \to \mathfrak{Q}_2$, *обмежені часом роботи* t *називатимемо однаковими (*$A_t = A'_t$*), якщо* $P\{A_t(l) \neq A'_t(l)\} < \varepsilon(t)$, $l \overset{rand}{\in} \mathfrak{Q}_1$.

Теорема 1 *(необхідна умова наявності каналу витоку). Якщо в протоколі 4 існує канал витоку, то* $\exists A_t, A'_t: V \to U$, $A'_t \neq A_t$, *що* $P\{D_t(v, A_t(v)) = 1\} > 1 - \varepsilon(t)$ *і* $P\{D_t(v, A'_t(v)) = 1\} > 1 - \varepsilon(t)$.

Доведення. Доведення конструктивне. Розглянемо алгоритми $A_0^\omega(v) \equiv A^\omega(v, 0)$ та $A_1^\omega(v) \equiv A^\omega(v, 1)$, $v \in V$. Тоді виконуватимуться умови теореми:

1. $P\left\{D_t\left(A_0^\omega(v)\right) = 1\right\} > 1 - \varepsilon(t)$ та $P\left\{D_t\left(A_1^\omega(v)\right) = 1\right\} > 1 - \varepsilon(t)$. Дійсно, згідно з визначенням 5 накладається вимога на непомітність каналу, тобто $\varepsilon(t) > Adv(A_1^\omega, A_t) \geq P\left\{D_t\left(A_t(v)\right)\right\} - P\left\{D_t\left(A_1^\omega(v)\right)\right\} = 1 - P\left\{D_t\left(A_1^\omega(v)\right)\right\} \Rightarrow P\{D_t(A_1^\omega(v))\} > 1 - \varepsilon(t)$ (для A_0^ω доведення аналогічне).

2. $A_0^\omega \neq A_1^\omega$. Доведемо від супротивного: нехай $A_0^\omega = A_1^\omega$, тоді $P\{A^\omega(v, 0) = A^\omega(v, 1)\} = 1 - \sigma, \sigma \in [0, \varepsilon(t))$ згідно з визначенням 6. Отже, $P\left\{R^\omega\left(A^\omega(v, s)\right) = 0\right\} = P\left\{R^\omega\left(A^\omega(v, s)\right) = 1\right\} = \frac{1}{2}$ з ймовірністю $p = 1 - \sigma$. З іншого боку, $P\{A^\omega(v, 0) \neq A^\omega(v, 1)\} = \sigma$ і тому $\max_s P\{R^\omega(A^\omega(v, s)) = s\} = \xi, \xi \in (1/2, 1]$. З цього слідує, що повна ймовірність буде

$$\max_s P\{R^\omega(A^\omega(v, s)) = s\} = \frac{1}{2}(1 - \sigma) + \xi\sigma = \frac{1}{2} + \sigma(\xi - \frac{1}{2}) \in [\frac{1}{2}, \frac{1}{2} + \frac{\varepsilon(t)}{2}),$$

що суперечить властивостям ймовірнісного алгоритму R_t^ω визначення 5.

Отже, алгоритми A_0^ω та A_1^ω є прикладами алгоритмів A'_t та A_t з умови теореми, тож теорема доведена конструктивно.

Наслідок. Нехай $\exists A_t, \forall v \in V: P\{D_t(v, A_t(v)) = 1\} = 1$ і $\forall A'_t: A'_t \neq A_t, P\{D_t(v, A'_t(v)) = 1\} = \sigma < 1 - \varepsilon(t)$. Тоді в протоколі неможливо побудувати канал непомітного витоку секрету. Більш того, у випадку передачі повідомлення секретним каналом, ймовірність виявлення факту цього складатиме $P \geq 1 - \sigma$.

Доведення. З $\exists A_t, \forall v \in V: P\{D_t(v, A_t(v)) = 1\} = 1$ і $\forall A'_t: A'_t \neq A_t, P\left\{D_t\left(v, A'_t(v)\right) = 1\right\} = \sigma < 1 - \varepsilon(t)$ випливає те, що $\forall A'_t, A''_t: A'_t \neq A''_t, P\{D_t(v, A'_t(v)) = 1\} < 1 - \varepsilon(t) \cup P\{D_t(v, A''_t(v)) = 1\} < 1 - \varepsilon(t)$, наслідком чого є достатня умова відсутності каналу непомітного витоку секрету.

Нехай сеанс передачі повідомлення характеризується двома властивостями: $Leak \in \{0,1\}$ – непомітний витік секрету відбувся та $Detect \in \{0,1\}$ – витік був виявлений. Тоді повна ймовірність виявлення факту витоку буде $P = P\{Detect = 1|Leak = 0\} + P\{Detect = 1|Leak = 1\}$. Але оскільки $P\{Detect = 1|Leak = 0\} = 0$ (неможливо виявити витік у випадку, якщо він не відбувся), то $P = P\{Detect = 1|Leak = 1\} \geq P\{Detect = 1\} = Adv(A_t, A'_t) \geq |P\{D_t(v, A_t(v)) - P\{D_t(v, A'_t(v))\}| = 1 - \sigma$.

Протокол генерації nonce. Протокол випадкового запиту nonce є базовим протоколом, що використовується майже у будь-якій системі аутентифікації для запобігання атак повторів.

Розглянемо базову схема протоколу випадкового запиту nonce.

Вихідні дані: абоненти Alice та Bob.

Кроки роботи протоколу:

1. Alice генерує унікальний одноразовий запит nonce та відправляє Bob.

2. Bob посилає відповідь "запит прийняв".

З точки зору клептографії, такий запит може слугувати контейнером з високою ємністю (немає чіткого обмеження на довжину nonce) для таємної передачі секрету Розробнику (у випадку зловмисної модифікації). З огляду на це, є ризик отримати канал витоку секретного ключа через запит.

Ця базова схема демонструє ідею використання схеми (див. рис. 1).

Нехай, в певному протоколі одним з кроків є передача випадкової послідовності (наприклад, як протидія до атак повторення у протоколах автентифікації). Якщо ця послідовність має довжину r бітів, то такий же розмір стегоконтейнеру ми отримуємо.

Вихідні дані:

1. Абоненти Alice та Bob.

2. Асиметрична криптосистема з простором K секретних ключів та простором Q публічних.

3. $Sign: K \times \{0,1\}^* \to B$ – функція генерації цифрового підпису без рандомізатору, B – простір підписів.

4. $Verify: Q \times \{0,1\}^* \times B \to \{0,1\}$ – функція перевірки цифрового підпису.

5. Пара асиметричних ключів абонента $(k_A, p_A), k_A \in K, p_A \in Q$.

6. $\psi: \{0,1\}^* \to \{0,1\}^*, \psi_0: Time \to \{0,1\}^*$ алгоритми генерації нового значення та ініціалізації лічильника.

Кроки роботи протоколу:

1. Абонент Alice обчислює наступне значення лічильника $ctr_i = \psi ctr_{i-1}$. Якщо попереднього значення не існує, можливе його створення, наприклад, на основі мітки часу $ctr_0 = \psi_0(time)$.

2. Абонент Alice обчислює $nonce = Sign(k_A, ctr_i)$ та передає значення $ctr_i|nonce$.

3. Bob перевіряє факт того, що не були задіяні власні джерела ентропії: $Verify(p_A, ctr_i, nonce) = = 1, ctr_i == \psi(ctr_{i-1})$.

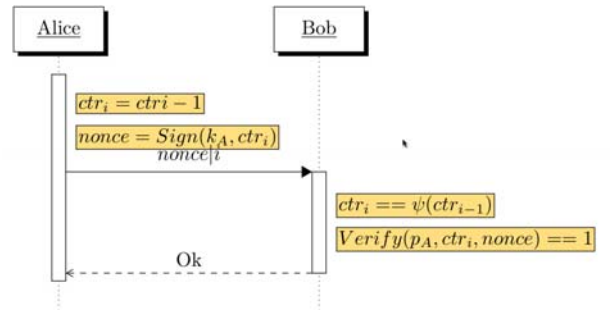

Рис. 1. Схема генерації nonce з викриттям стегоконтейнеру

Можливі зловмисні сценарії:

1. Зловмисник вгадує (прогнозує) випадкову послідовність до її публічної появи.

2. Зловмисник відновлює секретний ключ сторони А з перехоплених у відкритому каналі даних.

3. Розробник модифікує сторону А таким чином, щоб використовувати випадковий запит як стеганографічний контейнер.

У першому випадку, зловмиснику необхідно зі значень ctr_i та p_A отримати значення $Sign(k_A, ctr_i)$, тобто обчислити значення цифрового підпису без знання секретного ключа, що зводиться до задачі підробки цифрового підпису.

У другому випадку, зловмисник перехоплює відкриті дані: ctr_i, $Sign(k_A, ctr_i)$, p_A. На основі цих даних він має отримати секретний ключ k_A. Це можливо зробити або дискретним логарифмуванням публічного ключа (що зводиться до задачі пошуку секретного ключа за відомим публічним) або отримати його з відомого цифрового підпису (що зводиться до задачі пошуку секретного ключа цифрового підпису за значенням підпису та ключа перевірки).

У третьому випадку, алгоритм розробника задає значення випадкового запиту певним повідомленням (стеганограмою) M. Модифікація розробника також контролює секретний ключ k_A. Отже, модифікація розробника, маючи M (значення nonce) та k_A (секретний ключ підпису) має задати таке значення ctr_i, щоб $Sign(k_A, ctr_i) = M$. Перейдемо до більш загальної задачі: модифікація розробника, на основі M повинна згенерувати k'_A, R такі, щоб $Sign(k'_A, R) = M$ і $Verify(p_A, R, M) = 1$. Це також потребує розв'язання задачі підробки підпису.

Формалізуємо даний протокол, користуючись моделлю 5.

Визначення 7 *(протокол генерації випадкового запиту з викриттям стегоконтейнеру). Припустимо, абонент є оракулом Alice, сторона Bob займається викриттям каналу витоку.*

Протоколом генерації випадкового запиту з викриттям стегоконтейнера назвемо кортеж $\langle D_t, V, U, A_t \rangle$ моделі 4, де:

– V – множина можливих значень лічильника;

– U – множина можливих значень виходу абоненту;

– $A_t \equiv Sign(k_A, v)$, $v \in V$ – алгоритм абонента;

– $D_t \equiv Verify(p_A, v, u)$, $u \in U$.

Для оцінки клептографічної стійкості доведемо таку теорему.

Теорема 2 *(про відсутність SETUP у модифікованому протоколі генерації nonce). Нехай справедливе припущення:* $\forall v \in V$, $\forall A_t: A_t(k_A, v) \neq Sign(k_A, v)$, $P\{Verify(p_A, v, A_t(k_A, v)) = 1\} < \varepsilon(t)$ *(тобто, практично неможливо створити пару різних підписів одного повідомлення).*

Тоді у протоколі передачі випадкової послідовності 7 відсутній канал непомітного витоку секрету.

Доведення. В моделі 7 класифікатор $D_t \equiv Verify(p_A, v, u)$ задовольняє достатній умові наслідку теореми 1:

1. $\forall v \in V: P\{Verify(p_A, v, Sign(k_A, v)) = 1\} = 1$ за властивістю цифрового підпису.

2. $\forall v \in V, A_t(k_A, v) \neq Sign(k_A, v), P\{Verify(p_A, v, A_t(v)) = 1\} = \sigma < \varepsilon(t)$ за припущенням про практичну неможливість створення пари різних підписів.

Отже, за наслідком теореми 1, за наведених припущень, для протоколу в моделі 4 не існує каналу витоку секрету.

Більш того, у випадку передачі повідомлення прихованим каналом, ймовірність виявлення цього факту буде $P \geq 1 - \sigma \Leftrightarrow P > 1 - \varepsilon(t)$ за умови справедливості припущення теореми 2.

Модифікація протоколу Діффі-Хеллмана без SETUP

Протокол узгодження спільного ключа Діффі-Хелмана є базовим у багатьох системах захищеного зв'язку. Разом з тим, це один приклад криптосистеми, для якої Янг та Юнг розробили методи клептографічної модифікації з утворенням таємного каналу витоку з пропускною здатністю (1,2) [4]. Тож у даному розділі пропонується метод модифікації базового протоколу Діффі-Хелмана для узгодження спільного ключа з неможливістю модифікації з утворенням таємного каналу витоку відповідно до моделі 4.

Для ілюстрації ідей побудови каналу без витоку, використаємо як базовий однопрохідний протокол Діффі-Хеллмана.

Вихідні дані:

1. Абоненти Alice та Bob.

2. Асиметрична криптосистема для алгоритму Діффі-Хеллмана: G – генератор, K, Q – простір закритих та відкритих ключів $' \cdot ': K \times Q \to Q$ – функція узгодження (піднесення до степеню).

3. Симетричний шифр (E, D) з простором ключів S, та бієктивними функціями $E: S \times B \to B$, $D: \forall s \in S, \forall b \in B, D_s(E_s(b)) = b$.

4. Пара асиметричних ключів абонента Alice $(k_A, p_A), k_A \in \widetilde{K}, p_A \in \widetilde{Q}$.

5. Пара асиметричних ключів абонента Bob $(k_B, p_B), k_B \in K, p_B \in Q$.

6. Криптографічно сильні функції хешування $h1: B \to K$, $h2: Q \to S$.

Кроки роботи протоколу:

1. Абонент Alice генерує сесійний секретний ключ $q = Sign(k_A, ctr_i|Alice|Bob)$.

2. Alice відправляє відкритий сесійний ключ та ідентифікатори абонентів: $W = h1(q) \cdot G, (W, Alice, Bob) \to$ Bob.

3. Alice обчислює Симетричний (спільний) ключ каналу: $s = h2(h1(q) \cdot p_B)$.

4. Bob обчислює спільний симетричний ключ каналу: $s = h2(k_B \cdot W)$.

Розглянемо алгоритм встановлення захищеного каналу зв'язку між абонентами A та B за модифікованим протоколом Діффі-Хелмана, що дозволяє генерувати випадковий сесійний ключ каналу без можливості побудови прихованого каналу витоку SETUP (див. рис. 2). Вихідні дані:

1. Абоненти Alice та Bob.

2. Асиметрична криптосистема (цифровий підпис) з простором $\widetilde{K}$ секретних ключів та простором $\tilde{Q}$ публічних.

3. Асиметрична криптосистема для алгоритму Діффі-Хеллмана: G – генератор,K, Q – простір закритих та відкритих ключів $' \cdot ' : K \times Q \to Q$ – функція узгодження (піднесення до степеню).

4. Симетричний шифр (E, D) з простором ключів S, та бієктивними функціями $E: S \times B \to B$, $D: \forall s \in S, \forall b \in B, D_s(E_s(b)) = b$.

5. $Sign: \widetilde{K} \times \{0,1\}^* \to B$ – функція генерації цифрового підпису без рандомізатору, B – простір підписів.

6. $Verify: \tilde{Q} \times \{0,1\}^* \times B \to \{0,1\}$ – функція перевірки цифрового підпису.

7. Пара асиметричних ключів абонента Alice $(k_A, p_A), k_A \in \widetilde{K}, p_A \in \tilde{Q}$.

8. Пара асиметричних ключів абонента Bob $(k_B, p_B), k_B \in K, p_B \in Q$.

9. Криптографічно сильні функції хешування $h1: B \to K$, $h2: Q \to S$.

10. $\psi: \{0,1\}^* \to \{0,1\}^*$, $\psi_0: Time \to \{0,1\}^*$ алгоритми генерації нового значення та ініціалізації лічильника.

Кроки роботи протоколу:

1. Абонент Alice обчислює наступне значення лічильника $ctr_i = \psi ctr_{i-1}$. Якщо попереднього значення не існує, можливе його створення, наприклад, на основі мітки часу $ctr_0 = \psi_0(time)$.

2. Alice:

– Генерує сесійний секретний ключ $q = Sign(k_A, ctr_i|Alice|Bob)$.

– Симетричний ключ каналу: $s = h2(h1(q) \cdot p_B)$.

– Відправляє відкритий сесійний ключ, лічильник та ідентифікатори абонентів: $W = h1(q) \cdot G, (W, ctr_i, Alice, Bob) \to$ Bob.

3. Bob обчислює спільний симетричний ключ каналу: $s = h2(k_B \cdot W)$.

4. Alice відправляє свій секретний сесійний ключ закритим каналом: $E_s(q) \to Bob$.

5. Bob розшифровує ключ q. Перевіряє, чи дійсно цей ключ згенерований на основі публічної послідовності:

– Перевірка $ctr_i == \psi(ctr_{i-1})$. Якщо ні – лічильник не обчислений узгодженим алгоритмом, підозра на канал витоку, роз'єднання.

– Перевірка $h1(q) \cdot G == W$. Якщо ні – ключ недійсний, з'єднання розривається.

– Перевірка $Verify(p_A, ctr_i|Alice|Bob, q) = 1$. Якщо ні, то сесійний секретний ключ згенеровано не на основі відкритого лічильника, підозра на канал витоку, роз'єднання.

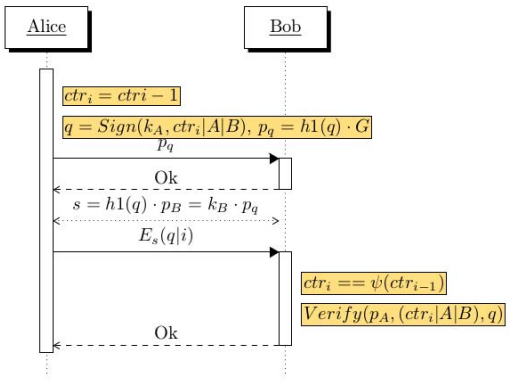

Рис. 2. Схема узгодження ключа Діффі-Хеллмана без каналу витоку

Можливі зловмисні сценарії:

1. Зловмисник (прогнозує) сесійний секретний ключ сторони $Alice$.

2. Зловмисник відновлює секретний ключ сторони $Alice$ з перехоплених у відкритому каналі даних.

3. Зловмисник – сторона Bob – намагається використати отриманий сесійний секретний ключ як свій секретний ключ для отримання спільного секрету з іншою стороною.

4. Розробник модифікує $Alice$ таким чином, щоб використати дані, що будуть відправлені до відкритого каналу, для організації непомітного витоку секрету (секретного ключа або сесійного секретного ключа).

Перші два сценарії розглядалися в 4.3.

У третьому випадку, сторона Bob отримує секретний сесійний ключ сторони $Alice$ під час роботи протоколу та потім намагається його використати для узгодження спільного секрету з іншою стороною (скажімо, сторона Dev). Проте тоді Bob має відправити разом з публічним ключем ідентифікатори $Alice$ та Bob, що сторона Dev розпізнає як недійсну сесію. У випадку ж, коли Bob відправляє ідентифікатори $Alice$ та Dev, сторона Dev викриває обман на етапі перевірки цифрового підпису: $Verify(p_A, (R_i|A|B), q)$

Нехай модифікація розробника має передавати певним чином закодований секрет до відкритого каналу. У випадку, якщо для цього будуть використовуватися додаткові відкриті повідомлення (окрім публічного ключа), це може бути виявлено зовнішнім спостерігачем, що порушує першу властивість SETUP (див. Визначення 3.1), а отже лазівка буде викрита.

Отже, у такому випадку, модифікація розробника може лише контролювати пару сесійних ключів (позначимо їх $(r, R), R = r \cdot G$), маючи при цьому доступ до секретного ключа k_A сторони $Alice$. Додаткові умови, які накладає протокол: $Verify(k_A, (S|A|B), r) = True$, де S – значення публічного лічильника. А це означає, що максимальна кількість можливих секретних ключів, що зможе згенерувати модифікація розробника дорівнює кількості практично згенерованих лічильників, а отже практично неможливо зафіксувати довільний секретний ключ.

Для формального доведення відсутності каналу непомітного витоку секрету, проведемо редукцію схеми до моделі 5.

Визначення 8 *(протокол узгодження спільного ключа без каналу непомітного витоку секрету). Розглянемо сеанс комунікації абонентів Alice (оракул) та Bob (він же займається викриттям каналу витоку).*

Протоколом узгодження спільного сесійного ключа без каналу непомітного витоку секрету назвемо кортеж $\langle D_t, V, U, A_t\rangle$ моделі 4, де:

– V – множина можливих значень лічильника;

– U – множина можливих значень виходу Alice;

– $A_t \equiv h1(q) \times G)|e$ – алгоритм абонента Alice, $q = Sign(k_A, v), e = E_s(q)$, $v \in V$;

– $D_t(v,u) \equiv Verify(p_A, v, getq(u)) * \mathbb{I}(getp(u) = h1\left(D_{gets(u)}(gete(u))\right) \cdot G$, $u \in U$, де функції $getq$, $getp, gets, gete$ обчислюються таким чином:

– $getp(u) = h1(q) \cdot G$;

– $gete(u) = e$;

– $gets(u) = h2(k_B \cdot getp(u))$;

– $getq(u) = D_{gets(u)}(gete(u))$.

Для оцінки клептографічної стійкості доведемо таку теорему.

Теорема 3 *(про відсутність SETUP у модифікованому протоколі узгодження ключа Діффі-Хеллмана).* Нехай справедливі припущення:

1. $\forall v \in V$, $\forall A_t: A_t(k_A, v) \neq Sign(k_A, v)$, $P\{Verify(p_A, v, A_t(k_A, v)) = 1\} < \varepsilon(t)$ (тобто, практично неможливо створити пару різних підписів одного повідомлення).

2. Функції $getq, getp, gets, gete$ обчислюються за час, яким можна знехтувати.

Тоді у протоколі 8 відсутній канал непомітного витоку секрету.

Доведення. Користуючись наслідком теореми 1 покажемо, що справджується достатня умова відсутності каналу витоку. В моделі 8 є класифікатор D_t який задовольняє достатній умові наслідку теореми 1:

1. $\forall v \in V: P\{D_t(p_A, v, A_t(v)) = 1\} = 1$. Дійсно, алгоритм D_t виглядає таким чином:

– Отримати $q, h1(q) \cdot G), s, e$ з u за допомогою функції $getq, getp, gets, gete$, ймовірність отримання правильних значень $p = 1$.

– Обчислити значення індикатору $\mathbb{I}(getp(u) = h1\left(D_{gets(u)}(gete(u))\right) \cdot G$. У випадку, якщо протокол проходить чесно, $h1(D_{gets(u)}(gete(u))) \cdot G) = h1(D_{gets(u)}(E_s(q))) \cdot G = h1(D_s(E_s(q))) \cdot G = h1(q) \cdot G$, тобто значення індикатору буде 1 з ймовірністю 1.

– Перевірити підпис $Verify(p_A, v, getq(u)) = Verify(p_A, v, q) = 1$ з ймовірністю 1 за властивістю цифрового підпису.

2. Нехай $A'_t \neq A_t$, тобто $\exists v \in V: A'_t(v) \neq A_t(v)$, $A_t(v) = g^{h1(q)}|e$, $A'_t(v) = g^w|e'$. Оцінимо ймовірність розпізнавання A'_t класифікатором D_t. В даному випадку можливі три ситуації:

– $h1(q) \cdot G \neq w \cdot G \wedge e = e'$. Тоді $s \neq s', s' = h2(w \cdot k_B \cdot G) \Rightarrow D_{s'}(e) = q' \neq q$, $P\{Verify(p_A, v, q') = 1\} < \varepsilon(t)$ (згідно з припущенням про практичну неможливість створення пари різних підписів одного повідомлення);

– $h1(q) \cdot G = w \cdot G \wedge e \neq e'$. Тоді $q' = D_s(e') \neq D_s(e)$ (в силу бієктивності функцій (E, D)), $P\{Verify(p_A, v, q') = 1\} < \varepsilon(t)$;

– $h1(q) \cdot G \neq w \cdot G \wedge e \neq e'$. Тоді $q' = D_{s'}(e')$. У випадку, якщо $q' \neq q$, $P\{Verify(p_A, v, q') = 1\} < \varepsilon(t)$. У випадку, якщо $q' = q$ ймовірність $P\{Verify(p_A, v, q') = 1\} = 1$. Згідо з протоколом, далі алгоритм D_t виконує перевірку $w \cdot G = h1(q') \cdot G$, що суперечить ситуації $h1(q) \cdot G \neq w \cdot G \wedge e \neq e'$.

Тож максимальна ймовірність $P\{D_t(v, A'_t(v)) = 1\} = \sigma < \varepsilon(t)$.

Отже, за наслідком теореми 1, за наведених припущень, для протоколу в моделі 4 не існує каналу витоку секрету.

Більш того, у випадку передачі повідомлення прихованим каналом, ймовірність виявлення цього факту буде $P \geq 1 - \sigma \Leftrightarrow P > 1 - \varepsilon(t)$ за умови справедливості припущення теореми 3.

Висновки

Наразі, проблеми клептографії для сучасних гібридних криптосистем є вкрай актуальні, а тому числі і за рахунок розповсюдження їхнього використання за межами захищених периметрів, що супроводжується недовірою до окремих абонентів. Більше того, абоненти, що стали жертвами клептографічних атак, можуть бути загрозою для системи комунікації в цілому.

Одним з напрямом клептографічних атак є SETUP – модифікація клептографічного протоколу у такий спосіб, що відбувається витік секретних ключів до Розробника, який виконав таку модифікацію, при чому інші учасники системи не здатні таку модифікацію виявити в процесі роботи. Тож основний фокус дослідження робиться на протидії таком типу атак, а саме, на побудову криптосистем з гарантованою відсутністю таких клептографічних модифікацій.

Слід зазначити, що під час досліджень зроблене базове припущення про те, що окремі криптопримітиви є стандартними та не містять додаткових клептографічних лазівок, лазівка впроваджується безпосередньо для реалізації конкретного абонента (жертви).

У ході проведених досліджень була розроблена формальна модель базового протоколу типу "запит-відповідь" та модель протоколу у клептографічному сенсі, що дозволило формалізувати великий клас криптографічних протоколів. Також сформульована та доведена теорема про достатні умови відсутності непомітного каналу витоку у криптопротоколі. Як демонстрація можливостей використання достатніх умов запропоновано два базових протоколи – генерація випадкового запиту nonce та модифікацію протоколу Діффі-Хеллмана узгодження ключа, а також сформульовані та доведені теореми про відсутність каналів витоку у даних протоколах.

Головним недоліком модифікації протоколу Діффі-Хеллмана є послаблення деяких криптографічних властивостей, зокрема прямої та зворотної секретності (forward and backward secrecy). Подальшими шляхами розвитку досліджень є побудова ряду стійких до SETUP модифікацій для розповсюджених теоретичних та практичних протоколів, а також покращення криптографічних властивостей протоколів без лазівок.

Література

[1]. A. Atanasiu, R. Olimid, E. Simion, "On the security of black-box implementation of visual secret sharing schemes", *Journal of Mobile, Embedded and Distributed Systems*, no. 4(1):1-11, 2012.

[2]. Côme Berbain and Henri Gilbert, "On the security of iv dependent stream ciphers", *Fast Software Encryption*, pp. 254-273, 2007.

[3]. A. Young, M. Yung, "The Dark Side of "Black-Box" Cryptography or: Should We Trust Capstone?", pp. 89-103, 1996.

[4]. A. Young, M. Yung, "Kleptography: Using Cryptography Against Cryptography", pp. 62-74, 1997.

УДК 004.056.523:57.087.1

Коваленко Б. Построение криптографических протоколов свободных от клептографических модификаций

Аннотация. *С широким распространением гибридных криптосистем в информационно телекоммуникационных системах, особую остроту приобретают задачи защиты данных криптосистем на всех уровнях жизненного цикла. Одной из характеристик современных криптосистем является распространение их использования в том числе и в слабо защищенных устройствах, что порождает новые векторы атак, в частности клептографических атак, например, с модификацией реализации криптосистемы на конечном устройстве. Такие типы атак особенно опасные, учитывая тот факт, что жертва злоумышленника, будучи частью определенной защищенной системы (электронного документооборота, платежной системы, секретной связи и т.п.), может нести угрозу также для нескомпрометированных участников системы (например, утечка совместных секретных данных). Одним из направлений решения этой проблемы является построение криптосистем, устойчивых к различным типам клептографических атак. Учитывая это, в статье изложены результаты по построению криптографических протоколов, устойчивых к атакам клептографической модификации реализации. Сначала строится формальная модель протокола типа ''запрос-ответ'' (''challenge-response'') с клептографическим каналом утечки секрета (subliminal channel). На основе предложенной модели определяются достаточные условия, при которых канал незаметной утечки не может быть построенным, формулируется и доказывается теорема о достаточных условиях отсутствия клептографического канала утечки. Также в статье предлагаются модификации двух базовых протоколов - генерации nonce и 1-проходной протокол согласования совместного ключа Диффи-Хеллмана, построенные с учетом достаточных условий. На основе формализации предложенных модификаций были сформулированы и доказаны теоремы об отсутствии клептографических каналов утечки в данных протоколах. Приведенные результаты могут быть использованы для построения других протоколов с доказанным отсутствием скрытых каналов утечки, что помогает решить одну из практических клептографических задач для повышения общей безопасности криптосистемы.*

Ключевые слова: *клептография, SETUP, каналы незаметной утечки секрета, протокол Диффи-Хеллмана, гибридная криптосистема, subliminal channel, challenge-response protocol.*

Kovalenko B. Development of SETUP-free cryptographic protocols

Abstract. *Today, hybrid cryptosystems are important part in structure of information telecommunication systems. That's why information security measures are extremely crucial at each stage of cryptosystem development life cycle. One of the most important specific of modern cryptosystems is the fact, that they often deployed in unprotected environment and outside the physically secured perimeter. That introduces new attack vectors, e.g. kleptographic attacks which include implementation forgery at endpoints. Such attack types are extremely dangerous because of the victim, who is a participant of some restricted area (electronic document flow, payment system, secure communication etc.), may induce threats for non-compromised participants (e.g., sensitive information leakage). One of the ways to solve mitigate this risks is development subliminal channel free cryptosystems which are resistant against different types of kleptographic attacks. In the article we show results belong to development of SETUP free cryptographic protocol development. Firstly, we suggest formal model for basic ''challenge-response'' protocol with subliminal channel. Using this formal model, we introduce sufficient conditions which lead to impossibility of existence of subliminal channels. Also the theorem about sufficient conditions has been formulated and proved. Further, we suggest improvements of basic protocols -- nonce generation and 1-round Diffie-Hellman key agreement protocol with design that is based of sufficient conditions. Using formalization of suggested enhanced protocols we formulated and proved the theorem about SETUP resistance property for these protocols. Our results may be useful for other SETUP free protocols development, this will be helpful for increasing security of hybrid cryptosystem.*

Keywords: *kleptography, SETUP, Diffie-Hellman key agreement, hybrid cryptosystem, subliminal channel, challenge-response protocol.*

Отримано *25 травня 2019 року*, затверджено редколегією *17 червня 2019 року*