DESMEDT AND A. M. ODLYZKO, "A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes", Advances in Cryptology–CRYPTO '85 (LNCS 218), 516–522, 1986. **12.** B. A. LAMACCHIA AND A. M. ODLYZKO, "Computation of discrete logarithms in prime fields", Designs, Codes and Cryptography, 1 (1991), 47–62. **13.** Smith P. and Skinner C. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms // In Advances in Cryptology, Asiacrypt '94, Springer-Verlag. - 1995. - Pp. 357-364. **14.** Bleichenbacher D., Bosma W., and Lenstra A. Some remarks on Lucas-based cryptosystems // In Advances in Cryptology, Crypto '95, Springer-Verlag. - 1995. - Pp.386-396. **15.** Маркушевич А. И. Возвратные последовательности. - М.: Наука, 1975. - 48 с. **16.** Яремчук Ю. Є. Методи та засоби шифрування інформації на основі рекурентних послідовностей. – Дис. ... канд. техн. наук: 05.13.21 – К., 2000. – 179 с. **17.** Яремчук Ю. Є. Криптографічні методи та засоби шифрування інформації на основі рекурентних послідовностей : Монографія. – Вінниця : Книга-Вега, 2002. – 136 с. **18.** Яремчук Ю. Є. Використання рекурентних послідовностей в задачах криптографічного захисту інформації // Захист інформації – 2002 – №6. – С. 37–45.

УДК 681.3.06

МОДЕЛІ БЕЗПЕКИ ДЛЯ ПРОТОКОЛІВ УЗГОДЖЕННЯ КЛЮЧІВ, ЩО ЗАСНОВАНІ НА ВЛАСТИВОСТІ НЕРОЗРІЗНЕНОСТІ

Олексій Мелецький
Харківський національний університет радіоелектроніки

Анотація: **Розглядаються моделі безпеки для протоколів узгодження ключів на базі нерозрізненості. Проводяться порівняння існуючих моделей, визначаються недоліки моделей та даються рекомендації щодо використання.**
Summary: **The indistinguishability-based security models of key agreement protocols reviewed. In this report we review and make a comparison of existing security models, checking the flaws and a recommendation offers.**
Ключові слова: **Протокол узгодження ключів, модель безпеки.**

I Вступ

Загальні визначення протоколів узгодження ключів

Головним предметом розгляду даної роботи є моделі безпеки для протоколів узгодження ключів, які задовольняють певним критеріям безпеки. Щоб протокол міг мати практичне застосування, він повинен бути безпечним. Тому для початку дамо визначення терміну «безпечний протокол» [1].

Визначення 1. *Безпечний протокол – це розподілений алгоритм взаємодії, який визначає послідовність кроків точно визначених дій, в яких беруть участь дві або більше сторін з метою досягнення певних цілей безпеки.*

За визначені дії протоколу зазвичай приймаються відправлення та отримання повідомлень, які реалізуються на базових криптографічних примітивах. До базових криптографічних примітивів відносять такі: шифрування, цифровий підпис та гешування [2, 3]. У кожного протоколу є послідовність взаємодії між користувачами протоколу, тобто поведінка кожної сторони протоколу узгодження ключів може бути описана алгоритмом, який виробляє вихідні данні у відповідь на вхідні дані [4]. Для вхідних даних найбільш характерними є наступні дані – короткотермінові секрети (наприклад, сеансові ключі), довгострокові секрети (довгострокові ключі користувачів, майстер ключі уповноваженого), загальносистемні параметри, вхідні повідомлення та інші дані. Вихідні дані – це вихідні повідомлення, результати виконання протоколу, встановлені секрети.

В сучасній криптографії протоколи узгодження ключів відіграють одну з головних ролей, це базовий елемент при побудові безпечних, складних, багаторівневих протоколів та криптографічних систем. Жодна криптографічна система, яка претендує називатися захищеною, не може обійтися без розподілення та узгодження ключів.

Визначення 2. *Протокол узгодження ключів [5] – це механізм, який дає змогу двом або більше сторонам взаємодії узгодити спільну таємницю, діючи при цьому в мережах зв'язку, які повністю контролюються порушником.*

Зазвичай, спільна таємниця встановлюється кожний раз при здійсненні протоколу (сесія). Протокол узгодження ключів забезпечує автентифікацію [1], якщо в протоколі всі сторони повністю впевнені в тому, що в розподіленні ключів беруть участь лише уповноважені та ідентифіковані сторони.

Визначення 3. Автентифікованим протоколом узгодження ключів [5] називається протокол узгодження ключів, який забезпечує всесторонню автентифікацію.

Визначення 4. *Автентифікованим протоколом узгодження ключів з підтвердженням [5] називається протокол узгодження ключів, який забезпечує обопільну (всіх сторін) автентифікацію та підтвердження ключів.*

Треба відмітити, що протоколи узгодження ключів не можуть здійснюватись без довіреної третьої сторони або уповноваженого [6]. Сучасні протоколи можна поділити за принципом взаємодії та роботи на дві великі групи. Перша група протоколів узгодження ключів – це протоколи з постійним використанням уповноваженого при кожному узгодженні ключів, для них є необхідність у постійному зв'язку з уповноваженим. Зазвичай, такі протоколи використовують симетричну криптографію. Прикладом є протокол Kerberos [7]. Друга група протоколів – це протоколи з використанням уповноваженого при потребі, наприклад, тільки при реєструванні користувача в системі. В таких протоколах використовується асиметрична криптографія. Як приклад можна привести протокол SSL [8].

Історично сформувалася група протоколів, на базі яких створюються більшість нових протоколів, в тому числі на базі ідентифікаторів. Сюди можна віднести наступні протоколи: Needham-Schroeder, Kerberos, Diffie-Hellman, MTI, MQV [9].

Існуючі проблеми створення безпечних протоколів узгодження ключів

Перед розробниками протоколів узгодження ключів завжди одним з найголовніших питань є впевненість у високому рівні безпеки протоколу, що створюється. Незважаючи на деяку простоту будова протоколів узгодження ключів, як здається на перший погляд, надати доказ безпеки протоколу, який би не мав недоліків та вразливостей, дуже важко. Прикладами можуть служити багато протоколів, які згодом виявилися нестійкими з різних причин [10 – 13]. Їхня кількість значно більша за протоколи, які є стійкими та витримали перевірку часом. Багато з протоколів, незважаючи на представлений доказ безпеки, стають непридатними для практичного використання в дуже короткий термін після їх представлення криптографічному співтовариству.

Розглянемо причини такої ситуації.

По-перше, відмітимо *різноманітність та чисельність різних умов (середовищ)* застосування порівняно з такими криптографічними примітивами як, наприклад, шифрування та цифровий підпис. В табл. 1 наведені відповідні дані.

Таблиця 1 – Порівняння критеріїв застосування протоколів узгодження ключів

Цифровий підпис та шифрування	**Протоколи узгодження ключів**
1. Алгоритми з чіткими покроковими діями	1. Алгоритми з інтерактивним характером взаємодії
2. Обмежена кількість атак	2. Існує багато різних видів та типів атак, кількість яких постійно збільшується
3. Залучена 1 сторона	3. Залучено, як мінімум, 2 сторони (3, якщо враховувати уповноваженого)

Протокол не існує в вакуумі і, зазвичай, є одним з багатьох елементів великої системи, безпека якої має бути забезпечена. Можлива ситуація, коли протокол сам по собі є коректним та безпечним при використанні його окремо від системи. Але він може бути некоректним та небезпечним при використанні як одного з елементів системи безпеки.

З наведеного можна зробити висновки, що головними причинами появи нестійких протоколів є:

- недооцінка або неправильне визначення можливостей порушника;
- неправильне формулювання цілей безпеки;
- неправильне формулювання вимог до криптографічних примітивів.

Історія розвитку протоколів показує, що з самого початку і до сьогоднішнього дня набір цілей та вимог до протоколів поповнюється та розширюється. Так, історично існує певний кругообіг – *створення нових протоколів приводило до появи нових атак, нові атаки, в свою чергу, потребували висування нових цілей безпеки та вимог до протоколів*. Така ситуація пояснюється недостатньою формалізацією моделей протоколів.

Тому застосування формальних моделей безпеки та доказ безпеки при створенні нових протоколів

узгодження ключів є дуже важливим, адже при правильному доказі можна уникнути появи недоліків безпеки та створити стійкий до існуючих атак та безпечний протокол.

Наразі існує два основних* різновиди в підходах конструювання моделей безпеки (рис. 1). Це моделі, які використовують підхід комп'ютерної безпеки [16], закладен в [4], та підхід на базі складності обчислення [17 – 20], що є предметом нашого розгляду. Підхід на базі складності обчислення є на даний час значно більш вживаниш на практиці через більш чітке визначення моделі та простіше практичне застосування. Тому дамо визначення дуже важливому терміну [21], який безпосередньо відноситься до підходу на базі складності обчислення.

Визначення 5. *«Нерозрізненість» (у випадку моделей безпеки) визначає вимогу, згідно з якою, порушник за поліноміальний час не зможе розрізнити між собою узгоджений спільний секрет (сесійний ключ) та випадкову послідовність.*

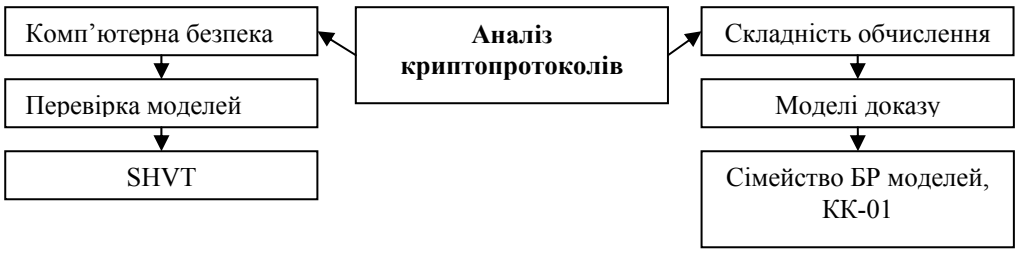

Рисунок 1 – Основні підходи до аналізу криптопротоколів

Вимоги до протоколів

До сучасних протоколів узгодження ключів висуваються багато різноманітних вимог. По-перше, базова вимога яка характеризує смисл самого узгодження ключа. Її можна визначити як *неспроможність обчислення установленого секрету без знання деяких секретних даних користувачів*. По друге, на сучасному етапі в галузі протоколів узгодження ключів сформовано вимоги, які припускаються за умовчанням, що кожний новий протокол повинен забезпечувати як обопільну автентифікацію, так і в деяких випадках підтвердження ключів.

Додаткові основні вимоги до протоколів узгодження ключів були сформульовані в роботах [1, 3, 21].

1. *Відома криптографічна живучість*. Компрометація одного сеансового ключа не повинна компрометувати ключі, які були встановлені в інших сесіях.
2. *Стійкість до невідомого ключового розподілення.* Неможливість розподілення ключа між користувачами A та C, якщо A має впевненість, що розподіляє ключі з B.
3. *Контроль ключових даних*. Жодна зі сторін протоколу не може створити чи вплинути на створення ключових даних за допомогою попередньо встановлених значень.
4. *Стійкість до компрометації ключа.* Компрометація довгострокового ключа сторони A не дає змогу порушнику видавати себе за інші сторони сесії.
5. *Попередня безпечність.* Якщо особистий (таємний) ключ одного з користувачів був скомпрометований, то безпечність сеансових ключів попередньо встановлених сесій не повинна бути зменшена.

Представлені вимоги до протоколів узгодження ключів є основними та дійсними для впровадження до більшості протоколів. Але до деяких протоколів висуваються інші вимоги, які пов'язані зі специфікою протоколів, що більш докладно визначені в [22, 23].

Історія розвитку моделей, заснованих на нерозрізненості

У 1993 році авторами (Bellare, Rogaway) роботи [19] був запропонований підхід до розподілення ключів, який містив в собі перше формальне визначення моделі порушника, яке було об'єднане з визначенням безпеки (для скорочення модель безпеки, яку запропонували Bellare Rogaway, будемо позначати, як БР-93). Модель визначала вороже середовище з обов'язковим існуванням порушника, який може застосовувати всі види атак (в тому числі і активні), перш за все такі, як зміна повідомлень,

* *Відомі дебати та критичні висловлювання щодо підходів до аналізу криптопротоколів. Ситуація така, що через різні базові положення* [14] *щодо криптографічних перетворень дослідники не мали між собою зв'язку та порозуміння. Але в останні роки ситуація стала покращуватися. Так, наприклад, в 2004 році Choo зробив спробу* [15] *уніфікації. Ним був запропонований «додатковий» підхід до аналізу криптопротоколів.*

розкриття спільного секрету та інші. БР-93 була визначена для двосторонніх протоколів узгодження ключів, які базуються на симетричній криптографії. Дана робота є базовою для моделей безпеки і в свій час спонукала не тільки до створення більш досконалих і спеціалізованих моделей, а і до різних поширень, за допомогою яких була формалізована безпека таких видів протоколів: двосторонні протоколи узгодження ключів на базі асиметричної криптографії, автентифіковані протоколи узгодження ключів з довіреною стороною (уповноваженим), автентифіковані протоколи узгодження ключів з поширеними властивостями безпеки та інші. Згодом в 1995 році Bellare та Rogaway провели аналіз протоколу трьохстороннього розподілення ключів [20], використовуючи розширену модель БР-93 (позначимо, як БР-95), яка була виправлена, бо Rackoff знайшов в моделі БР-93 помилки [5] та доповнена з урахуванням конкретного типу протоколів. Але найбільш уніфікована модель була представлена в 2000 році, авторами якої були Bellare, Pointcheval та Rogaway (БПР-00) [18]. Тому моделі БР-93, БР-95 та БПР-00 можна згрупувати як сімейство моделей Bellare-Rogaway.

Окремо необхідно виділити модель КК-01 [24], що була представлена в 2001 році авторами Canetti-Crawczyk. Модель базується на роботі [17], в якій запропоновано дещо інший підхід до визначення та формалізації безпеки протоколів узгодження ключів. Ключовим елементом такої моделі є модульний підхід, що має декілька вагомих переваг. Незважаючи на відмінність ця модель має багато спільного з моделями БР.

Головними цілями даної роботи є:

- визначення проблемних питань створення безпечних протоколів узгодження ключів;
- визначення загальних вимог до протоколів узгодження ключів;
- опис існуючих моделей безпеки на базі нерозрізненості;
- порівняння моделей безпеки на базі нерозрізненості;
- визначення основних недоліків та вироблення рекомендацій для моделей безпеки на базі нерозрізненості.

II Моделі безпеки, що засновані на нерозрізненості

Загальні питання моделей безпеки

Розглянемо сутність сімейства моделей Bellare-Rogaway. Відмітимо, що представлені базові елементи мають багато спільного також з моделлю КК-01 [24].

Для протоколів узгодження ключів сесія є базовим зображенням поточного стану. Оракул є базовим елементом моделі, до якого залучені користувачі, що беруть участь в сесії протоколу. Базова модель має набір U_1, ..., U_m користувачів протоколу. Протокол визначає правила, як користувачі повинні вести себе на відповідь вхідним сигналам з середовища протоколу. Кожна сторона протоколу може виконати сесію протоколу багато разів з будь-якими партнерами. Поведінка кожного з користувачів моделюється в вигляді оракула $\Pi^i_{U_1U_2}$, який моделює виконання користувачем U_1 сесії з користувачем U_2 в протоколі встановлення розподіленої таємниці. Оракул зберігає всі повідомлення, які він відіслав та отримав від користувачів.

Також введемо модель порушника Λ, який контролює всі комунікаційні зв'язки між взаємодіючими сторонами. Порушник може перехопити всі оракули взаємодії та зробити до них запити. Порушник Λ в будь який час може виконати наступні запити :

- $Send(U_1, U_2, mess, i)$. Цей запит дозволяє Λ відіслати деяке повідомлення, на вибір порушника, зі змістом $mess$. Вихідні дані (повідомлення або рішення) оракула $\Pi^i_{U_1U_2}$ надсилаються порушнику Λ. Якщо оракула $\Pi^i_{U_1U_2}$ не існує, то він може бути створений. Порушник може запросити користувача U_1 встановити сесію з користувачем U_2 відсилаючи запит $Send(U_1, U_2, \lambda, i)$, де λ пусте повідомлення, тобто може бути ініціатором взаємодії (той, хто відсилає перше повідомлення в поточній сесії). Цей запит дає змогу порушнику видати себе за іншого користувача протоколу.

- $Reveal(U_1, U_2, i)$. Запит дозволяє Λ викривати сесійні ключі, затверджені в минулому.

- $Corrupt(U_1, K_E)$. Запит дозволяє Λ викривати довгострокові закриті ключі.

- $Test(U_1, i)$. Запит можна виконувати тільки тоді, коли оракул знаходиться в стані *Accepted*. Відповіддю на даний запит є випадковий біт b. Якщо біт b дорівнює 0, то на виході випадкове значення сесійного ключа. В іншому випадку на виході дійсний сесійний ключ. Порушник може здійснити запит

лише один раз протягом всієї сесії, або життєвого циклу оракула.

Всі користувачі протоколу, які беруть участь в одній і тій же сесії при розподіленні ключів, повинні отримати і узгодити однаковий ключ. Також необхідно відмітити, що кожна сторона протоколу діє за заздалегідь визначеними кроками, які встановлені протоколом. Кожного оракула $\Pi^i_{U_1U_2}$ можна представити в вигляді послідовності повідомлень $Conv = (\tau_1, \alpha_1, \beta_1), (\tau_2, \alpha_2, \beta_2), ..., (\tau_m, \alpha_m, \beta_m)$, при умові, що $\tau_s < \tau_{s+1}$, тобто час τ_{s+1} є більш пізнім, ніж час τ_s. Послідовності повідомлень $Conv$ можна визначити за час τ_s, якщо оракул $\Pi^i_{U_1U_2}$ отримав запит α_s та відповів β_s. На рис. 2 представлена послідовність перетворень, що погоджуються [5].

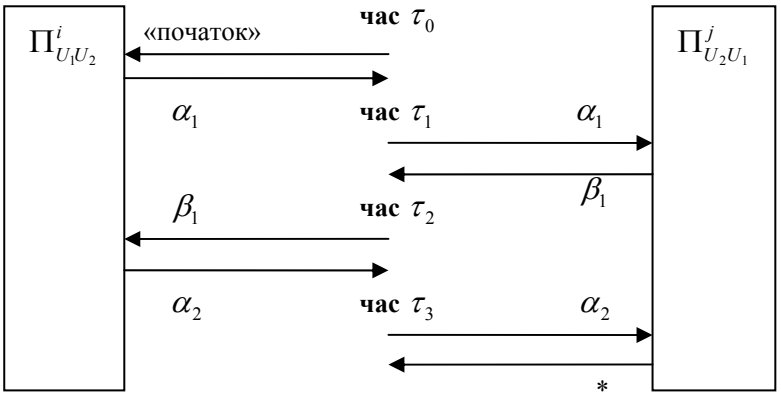

Рисунок 2 – Перетворення, що погоджуються

Визначимо також два важливих терміни – партнера та сесійного ідентифікатора.

Визначення 6. *Сесійний ідентифікатор – це інформація, яка використовується сторонами протоколу для однозначної ідентифікації сесії. Два оракула,* $\Pi^i_{U_1U_2}$ *та* $\Pi^j_{U_1U_2}$, *протоколу* Π *мають перетворення, що погоджуються, якщо вони отримали однаковий сесійний ідентифікатор.*

Визначення 7. Два оракула можуть бути партнерами, якщо виконуються наступні дві вимоги:

- вони мають однаковий сесійний ідентифікатор p;
- імовірність того, що дві сесії мають однаковий сесійний ідентифікатор, є незначною.

Модель на базі оракулів дає змогу симулювати середовище виконання протоколу разом зі всіма загрозами. В такій моделі існує порушник, якому даються необмежені можливості в доступі до мережі взаємодії користувачів. Крім того, порушник може бути представлений не тільки як третя сторона, яка діє ззовні, а і як внутрішньосистемний користувач, що діє з легітимними правами на доступ до довгострокового ключа. Порушнику також дається право контролювати (знати) моменти генерації випадкових значень сторін протоколу. Визначення безпеки в такій моделі є дуже важливим моментом для самої моделі.

Для порушника одним з головних завдань є отримання значення сеансового ключа. В моделі з секретними повідомленнями оракули, наприклад, з сеансовими ключами, можуть бути визначені порушником наступним чином: через прямий запит $Reveal$, або через отримання довгострокового секрету через запит $Corrupt$. Головним завдання є забезпечення унеможливлення визначення порушником таких оракулів, які містять секретні значення. Тому для цього введемо визначення «нового оракула».

Визначення 8. Оракул $\Pi^i_{U_1U_2}$ *вважається новим, або має новий сеансовий ключ в кінці життєвого циклу, якщо :*

1) оракул $\Pi^i_{U_1U_2}$ *знаходиться в стані Accepted та містить сеансовий ключ;*

2) до оракула $\Pi^i_{U_2U_1}$ *не було запитів типу Reveal або Corrupt, тобто, оракул не був атакований порушником;*

3) не існує оракула $\Pi^{t}_{U_1U_2}$ *до якого не було здійснено запит Reveal (для моделі КК-01 також запит Reveal, який будемо в подальшому визначати, як Reveal2, який стосується не тільки сесійного ключа, а й всього поточного стану), та який має перетворення, що пого*джуються з оракулом $\Pi^{i}_{U_1U_2}$.

Безпеку можна визначити як модель взаємодії (гру) Γ між порушником Λ та набором оракулів $\Pi^{i}_{U_XU_Y}$ для користувачів $U_X, U_Y \in \{U_1, U_2, ..., U_{N_P}\}$, де $i \in \{1, ..., N_S\}$. Схема такої взаємодії, представлена на рис. 3.

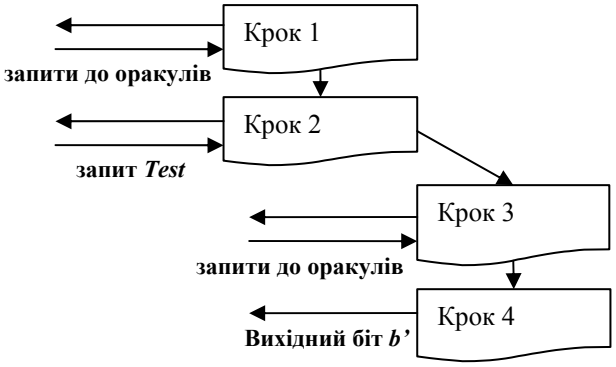

Рисунок 3 – Схема взаємодії

Крок 1. На цій стадії взаємодії порушник має можливість робити, за бажанням, будь-які наступні запити **Send**, **Reveal (Reveal2)** або **Corrupt**.

Крок 2. Порушник в будь-який момент взаємодії Γ вибирає сесію з новим оракулом та відсилає запит **Test**, для зв'язування оракула з сесією, яка тестується. При цьому вибрана сесія має бути новою. При розподілі сесійного ключа залежно від випадково вибраного біту **b**, порушник отримує справжній сеансовий ключ або випадкову послідовність.

Крок 3. Цей крок подібний першому, коли порушник продовжує робити за бажанням запити типу **Send**, **Reveal (Reveal2)** або **Corrupt.**

Крок 4. В заключній стадії порушник закінчує взаємодію, отримує біт **b'** та робить припущення щодо змісту біту **b.**

Успіх порушника в Γ при спробі атаки можна визначити за допомогою терміну „успіху порушника" $Advantage_{\Lambda}(k)$, який характеризується отриманням реального ключа, чи набору випадкових даних. При атаці порушник Λ експериментує з набором оракулів та може зробити поліноміальну кількість запитів, включаючи один запит $Test$. Порушник отримує справжній ключ (виграє гру), якщо після запиту $Test(U_1, U_2, i)$, де оракул $\Pi^{i}_{U_2U_1}$ знаходиться в стані Accepted та є новим, порушник не має сумніву до еквівалентності значення бітів b' та b, які були отримані при запиті $Test(U_1, U_2, i)$.

Базова ідея нерозрізненості – це вимога, згідно з якою даний новий сеансовий ключ та випадкова послідовність, яка була згенерована згідно з тим самим розподіленням ключів, не може бути визначена (розрізнена) порушником в поліноміальний час з імовірністю більшою, ніж ½. Тому визначити успіх порушника Λ можна в вигляді функції [21]:

$Advantage_{\Lambda}(k) = 2\Pr[b = b'] - 1$, де k – секретний параметр.

Визначення 9. *Автентифікований протокол узгодження ключів є безпечним [19], якщо наступні властивості виконуються для будь-якого порушника:*

1. два оракула, $\Pi^{i}_{U_1U_2}$ та $\Pi^{j}_{U_2U_1}$, утримують однаковий сеансовий ключ, якщо вони не мали запитів $Corrupt$ з боки порушника та мають погоджені перетворення;

2. для всіх порушників протоколу значення $Advantage_{\Lambda}(k)$ є незначним.

Визначення 10. *Автентифікований протокол узгодження ключів з підтвердженням є безпечним [19], якщо виконуються такі вимоги:*

1. два оракула, $\Pi^i_{U_1U_2}$ *та* $\Pi^j_{U_2U_1}$ *, утримують однаковий сеансовий ключ, якщо до них не було запитів* $Corrupt$ *зі сторони порушника та використовують погоджені перетворення;*

2. незначна ймовірність для наступного випадку: $\Pi^i_{U_1U_2}$ *знаходиться в стані Accepted, але для нього немає оракула* $\Pi^j_{U_2U_1}$ *з перетвореннями, що погоджуються;*

3. Для всіх порушників протоколу значення $Advantage_\Lambda(k)$ *є незначним.*

Визначення автентифікованого протоколу узгодження ключів та автентифікованого протоколу узгодження ключів з підтвердженням визначають критерії безпечності протоколів.

Визначення 11. *Протокол не є безпечним, якщо виконуються наступні умови*:

1. *два нових оракула, які не є партнерами, мають однакові ключі (наприклад сеансові);*
2. *два нових оракули партнери, які знаходяться в стані Accepted, мають різні ключі;*
3. *деякий новий оракул, який знаходиться в стані Accepted та має деякий ключ, був атакований порушником* Λ *;*
4. *деякий новий оракул, який знаходиться в стані Accepted, закінчив свій життєвий цикл без оракула партнера.*

Специфіка моделі КК-01

Незважаючи на те, що модель КК-01 має певні збіги та схожість з моделями сімейства БР, вона має також деяку концептуальну відмінність.

Головною відмінністю є застосування модульного способу при доказі безпеки протоколу, який був запропонований в [24] на базі роботи [17]. Необхідно відмітити переваги модульного доказу безпеки, який дозволяє окремо провести доказ кожного з компонентів, та розділити розгляд автентифікації та обмін ключовими даними. Провівши доказ кожного компонента на безпечність, можна робити висновки з безпеки взагалі всього протоколу узгодження ключів. Таким чином, основними перевагами такого способу є спрощення доказу, більш висока стійкість до помилок при доказі, та можливість конструювання протоколів з певними вимогами під конкретні випадки на базі елементарних базових та безпечних компонентів.

Відмінність від моделей сімейства БР визначається також в типі моделі порушника. Так модель включає дві взаємодіючі моделі: це «реальна модель» без автентифікованих зв'язків – UM , та «ідеальна модель» з автентифікованими зв'язками – AM . UM модель більш близька до моделі реального світу, порушник має змогу діяти за правилами реального світу. Тобто порушник повністю контролює канали взаємодії між сторонами протоколу, та може застосовувати активні атаки – створювати нові, модифікувати, чи видаляти повідомлення. В ідеальній моделі більш жорсткі умови – порушник не має права створювати нові повідомлення та видаляти (не давати доходити до кінцевого користувача) повідомлення.

Особливістю моделі КК – 01, яка, до речі, дає можливість реалізовувати властивість модульності, є наявність автентифікатора. При цьому застосовується двохступеневий підхід (рис 4), в якому спочатку необхідно провести доказ безпеки протоколу узгодження ключів в ідеальному автентифікованому середовищі, тобто, AM , а потім, шляхом трансформації протоколу, зробити такий його варіант, який би був безпечним в реальному середовищі, тобто, UM . Зміна протоколу, зокрема шляхом зміни потоку повідомлень оригінального протоколу для AM , і є автентифікатором. Є очевидним, що доказ безпеки протоколу в моделі UM залежить від доказу безпеки [21] автентифікатора, який використовується, і якщо доказ безпеки буде спростований, то, очевидно, що і доказ безпеки всього протоколу в моделі UM буде спростований.

Рисунок 4 – Використання автентифікатора при побудуванні протоколів

Існує певний набір протоколів, які задовольняються вимогам ідеального середовища. Вони можуть стати базовими для побудови нових протоколів. До них можна віднести наступні протоколи: *Diffie-Hellman (побудований на базі вирішення проблеми DDH), Tripatite Diffie-Hellman (побудований на базі вирішення проблеми BDH), Key Transport, El Gamal (Gap DH),* та інші. Найбільш поширені автентифікатори [15] представлені в табл. 2.

Таблиця 2 – Найбільш поширені автентифікатори

Автентифікатори	Криптографічний примітив
На базі підпису	Цифровий підпис
На базі шифрування	MAC + шифрування
На базі пароля	Шифрування
На базі MAC	MAC
На базі статичного ключа	CDH + хешування

Великою перевагою модульного підходу є те, що елементи протоколу узгодження ключів, для яких був проведений доказ безпеки, можуть в подальшому служити будівельним матеріалом багаторазового використання для нових доказовобезпечних протоколів. Ще однією перевагою при будуванні нових протоколів на базі моделі КК-01 є гнучкість до змін. Протокол може мати певні властивості за бажанням, наприклад такі, як відома криптографічна живучість, стійкість до невідомого ключового розподілення та інші.

III Аналіз моделей безпеки

Види моделей безпеки та їх відмінність

На початку даної роботи була представлена коротка історична довідка про розвиток моделей безпеки. Необхідно чітко представляти різницю між ними, адже неадекватне вживання моделі доказу може призвести до появи вразливостей протоколів. Кожна з моделей має свою специфіку. Розкриємо найбільш важливі відмінності та дамо їм коротку характеристику.

Потужність порушника. Кожна з моделей розглядає різну потужність порушника, що добре представлено в табл. 3.

Таблиця 3 – Потужність порушника в модулях безпеки та їх порівняння

Запити до оракулів	БР-93*	БР-95	БР-00	КК-01
$Send(U_1, M)$	+	+	+	+

** Будемо використовувати удосконалену модель безпеки БР-93, яка дозволяє порушнику виконувати запит* $Corrupt(U_1, K_E)$*, незважаючи на те, що в оригінальній версії даного запиту немає.*

$Reveal(U_1, U_2, i)$	+	+	+	+
$Reveal2(U_1, U_2, i)$ **	-	-	-	+
$Corrupt(U_1, K_E)$	+	+	-	+
$Test(U_1, U_2, i)$	+	+	+	+

2. ***Партнерство.*** Партнерство оракулів та нерозрізненість сеансових ключів є важливими складовими в визначенні моделі безпеки протоколу. В моделі БР-93 визначення терміну партнерство базується на перетвореннях, що погоджуються. Модель безпеки БР-95 визначає термін партнерства на базі функції партнерства. Функція партнерства використовує набір всіх запитів типу $Send$ для визначення партнера оракула через відображення між двома оракулами, які розподіляють спільний секрет. Але таке визначення партнерства є вразливим, бо вказаний недолік може бути використаним [25]. Визначення партнерства оракулів через сеансовий ідентифікатор використовується в інших двох моделях безпеки БР-00 та КК–01. Для БР-00 визначення сеансового ідентифікатора здійснюється засобом конкатенації повідомлень протоколу. Навпаки для моделі КК–01 конкретного способу створення такого ідентифікатора не визначено. Але необхідно враховувати, що спосіб формування сеансового ідентифікатора може впливати на безпеку протоколу.

3. ***Модульний підхід до визначення моделі.*** Модель КК-01, на відміну від сімейства моделей БР, використовує модульний підхід до визначення безпеки. В попередньому розділі це детально розглянуто.

4. ***Забезпечення цілей безпеки.*** Всі моделі вимагають обґрунтування цілей безпеки.

Таблиця 4 – Цілі безпеки моделей безпеки та їх порівняння

Типи цілей	БР-93	БР-95	БР-00	КК-01***
Автентифікація (А)	+	-	+	+
Розподілення ключів(РК)	+	+	+	+

З табл. 4 можна сформувати набір варіантів моделей доказу для моделей сімейства БР. Кожний варіант може бути використаний для доказу безпеки протоколів (рис.5).

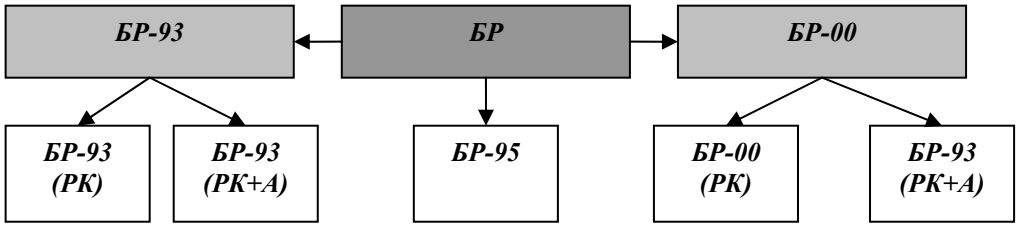

Рисунок 5 – Сімейство моделей доказу БР та їх варіанти

Взаємозв'язок доказів

Всі моделі, представлені в даній роботі, мають взаємозв'язок [21] між собою. Адже кожна з моделей має дуже багато спільного. Різниця виражається в деяких нюансах та визначеннях. І тільки модель КК-01 має більш значні відмінності. Незважаючи на це, можна зробити висновки, що протокол, для якого зроблено доказ безпеки в одній з моделей, може автоматично бути безпечним і в іншій моделі.

** *Запит* $Reveal2(U_1, U_2, i)$ *відрізняється від запиту* $Reveal(U_1, U_2, i)$ *більшою потужністю для порушника, адже окрім сеансового ключа порушник отримує весь стан користувача.*

*** *В представленій таблиці вміст моделі КК-01 не є зовсім доречним, так як модель базується на дещо других принципах та засадах. Недоречність неформального порівняння моделей було вказано в* [26].

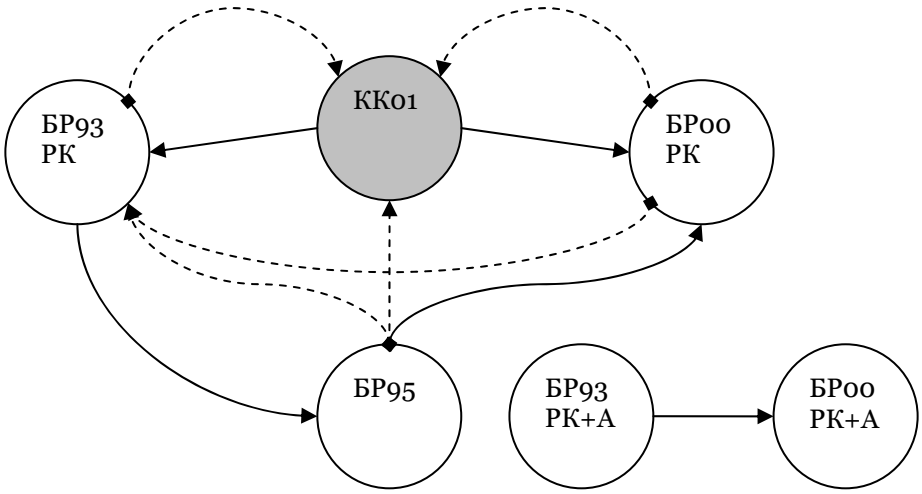

Рисунок 6 – Взаємозв'язок доказів

На рис. 6 показані моделі безпеки та відповідний взаємозв'язок між доказами. Суцільна лінія показує автоматичний доказ для іншої моделі, наприклад, доказ, який був проведений для моделі КК-01 автоматично стає безпечним і для моделей БР-93(РК) та БР-00(РК). Пунктирна лінія свідчить, що доказ в одній моделі не є автоматичним для інших, та, як мінімум, потребує узгоджень на рівні визначень між моделями. Наприклад, доказ, який був проведений для моделі БР-00(РК) потребує змін для доказу в моделях КК-01 та БР-93(РК).

Проблеми існуючих моделей

Роботи [17 – 20] зі створення моделей безпеки були значним успіхом в формалізації безпечних протоколів, що дало значний поштовх в їх розвитку. Але незважаючи на значне спрощення відносно формалізації протоколів та поширене використання моделі доказу на практиці, до вирішення всіх проблем ще досить далеко [27], та існує певна категорія проблем, які чекають свого вирішення. Перелік таких проблем для протоколів сімейства БР наведено нижче.

1. Проведення процесу доказу є достатньо довгим та складним. Існує багато прикладів з допущеними помилками при доказі безпеки протоколів узгодження ключів, що підтверджує його складність.
2. Сам процес доказу є негнучким. Він не може використовуватися як допоміжний засіб при конструюванні нових протоколів. Порівняно висока складність при повторному виконанні доказу. Навіть невелика зміна в протоколі змушує розроблювачів створювати заново модель доказу безпеки протоколу.
3. Досвід практичного використання моделей безпеки виявив іншу проблему [25], яка пов'язана з труднощами при доказі протоколів узгодження ключів без використання цифрових підписів.
4. Визначення перетворень, що погоджуються, є нерівнозначним та має певні недоліки. Це стосується деякої несиметричності при формуванні ключових даних. Наочний приклад наведений в [26].
5. Серед спеціалістів в галузі криптографії існує думка та впевненість щодо високої ймовірності існування ще не визначених помилок серед моделей сімейства БР, що є недоліком.
6. Використання моделей безпеки БР-93 та БР-95 в оригінальному вигляді є не доцільним, бо при визначені функції партнерства [18] були знайдені помилки [21]. До того ж, наведені приклади для використання моделей також мали помилки, які унеможливлювали отримання сеансового ідентифікатора. Це стосується протоколу 3PKD. В роботах [15, 25, 26] запропоновані методи виправлення помилок.

Незважаючи на поширене та успішне використання моделей безпеки при доказі протоколів на базі сімейства моделей БР, існування очевидних недоліків, що представлені вище, зводило нанівець докази багатьох протоколів. Тому, після того як був запропонований модульний підхід для моделей на базі нерозрізненості, стало очевидним, що він більш ефективний, ніж моделі БР. Тепер з'явилася можливість не тільки аналізувати створений протокол та вести для нього доказ безпеки, але й створювати нові безпечні протоколи за допомогою моделі КК-01. Такий підхід може нагадувати створення нових протоколів із елементів. Але, як показав практичний досвід, використання модель КК-01 є тільки певним

кроком до створення ідеальної моделі безпеки. Модель КК-01 також має свої недоліки та обмеження. До них можна віднести наступні.:

1. Проведення процесу доказу все ще є достатньо довгим та складним. Але необхідно відмітити, що в деяких випадках воні значно простіше, ніж для моделі БР.
2. Існує ряд протоколів, для яких немає адекватного відображення автентифікатора в UM , наприклад для протоколів з автентифікаторами на базі паролю [28].
3. Модель має обмежене практичне застосування. Не для всіх протоколів можна провести доказ на баз КК-01. Відмітимо, що завдяки роботі [29] обмеження значно скоротились.

IV Висновки

В статі розглянуто такі проблемні питання:

- Чи існують безпечні протоколи ?
- В чому сутність моделі безпеки?
- Які моделі безпеки необхідно використовувати залежно від вимог?

Основним висновком відносно протоколів узгодження ключів є визначення необхідності чітких доказів безпеки відносно існуючих активних атак в чітко визначеній моделі безпеки.

Проведене порівняння протоколів дало змогу дати такі рекомендації щодо виростання моделей. По-перше найбільш безпечним протоколом є той, для якого був зроблений доказ в моделі КК-01. Вона є найбільш потужна, адже надаються найбільш широкі можливості порушнику. Найбільш слабка з точки зору безпеки є модель БР-00. Необхідно пам'ятати, що протокол, для якого був зроблений доказ в одній з моделей безпеки, може не бути безпечним в іншій моделі.

Необхідно пам'ятати, що через відсутність доказу безпомилковості самих моделей безпеки існує також можливість знаходження вразливостей в протоколах, безпечність для яких вже доведена.

На наш погляд значних перспектив застосування БР моделей немає. Тому, по можливості, більшість доказів протоколів необхідно здійснювати для моделі КК-01. При цьому використання для доказу удосконаленої моделі [29] КК-01 є не тільки більш зручним та гнучким, але й надає найбільші гарантії безпеки самого протоколу від активних атак порушника.

Література: ***1.*** *A. Menezes, P. C. van Oorschot, S. Vanstone. Handbook of Applied Cryptography. CRC Press, July 1999.* ***2.*** *Krawczyk H., SKEME: A Versatile Secure Key Exchange Mechanism for Internet, in 'ISOC Network and Distributed System Security- NDSS 1996, IEEE Internet Society Press, pp. 114 – 127.* ***3.*** *M. Gorantla, R. Gangishetti, A. Saxena. A. Survey on ID-Based Cryptographic Primitives. http://eprint.iacr.org/2005/093.pdf* ***4.*** *Dolev D., Yao A. C. (1983), 'On the Security of Public Key Protocols', IEEE Transaction of Information Technology 29(2), 198 – 208.* ***5.*** *Z. Cheng, M. Nistazakis, R. Comley, L. Vasiu. On The Indistinguishability-Based Security Model of Key Agreement Protocols-Simple Cases. http://eprint.iacr.org/2005/129.pdf.* ***6.*** *V. Shoup. On Formal Models of Security Key Exchange. IBM Zurich Research Lab. Report.* ***7.*** *J. Steiner, C. Neuman, J. Schiller. Kerberos: An Authentication Service for Open Network Systems. 1988.* ***8.*** *SSL Protocol Version 3. 0 March 1996 http://wp.netscape.com/eng/ssl3/ssl-toc.html.* ***9.*** *A. Menezes, M. Qu, S. Vanstone. Some new key agreement protocols providing mutual implicit authentication, Second Workshop on Selected Areas in Cryptography (SAC95), 1995.* ***10.*** *O. Pereira, J. Quisquater. Some Attacks Upon Authenticated Group Key Agreement Protocols. Journal of Computer Security, 11:555 – 580, 2003.* ***11.*** *Z. Wan, S. Wang. Cryptanalysis of Two Password-Authenticated Key Exchange Protocols. 9th Australasian Conference on Information Security and Privacy. ACISP 2004. Springer-Verlag, 2004. Volume 3108/2004 of Lecture Notes in Computer Science.* ***12.*** *Duncan S. Wong, Agnes H. Chan. Efficient and Mutually Authenticated Key Exchange for Low Power Computing Devices. Advances in Cryptology - Asiacrypt 2001, pages 172 – 289. Springer-Verlag, 2001. Volume 2248/2001 of Lecture Notes in Computer Science.* ***13.*** *M. Zhang. Breaking an Improved Password Authenticated Key Exchange Protocol for Imbalanced Wireless Networks. IEEE Communications Letters, 9(3):276 – 278, 2005.* ***14.*** *C. Boyd. Design of Secure Key Establishment Protocols: Successes, Failures and Prospects. Information Security Research Centre, Queensland University of Technology, Springer-Verlag Berlin Heidelberg, 2004.* ***15.*** *K.-K. R. Choo, Y. Hitchcock. Security Requirements for Key Establishment Proof Models: Revisiting Bellare--Rogaway and Jeong--Katz--Lee Protocols. In 10th Australasian Conference on Information Security and Privacy - ACISP 2005, Brisbane, Australia, LNCS 3574/2005 (pp. 429 – 442), 04 - 06 Jul 2005.* ***16..*** *C. Meadows. Formal Methods for Cryptographic Protocol Analysis: Emerging Issues and Trends. IEEE Journal on Selected Area in Communications, 21(1), 2003.* ***17****. M. Bellare, R. Canetti, H. Krawczyk. A modular approach to the design and analysis of authentication and key exchange protocols. In 30th ACM Symposium on Theory of Computing, pages 419 – 428. ACM Press, 1998. 18. M. Bellare, D. Pointcheval, P. Rogaway. Authenticated Key Exchange Secure Against Dictionary Attacks. Advances in Cryptology – Eurocrypt*

2000, pages 139 – 155. Springer-Verlag.2000. ***19.*** *M. Bellare, P. Rogaway. Entity Authentication and Key Distribution. In Douglas R. Stinson, editor, Advances in Cryptology - Crypto 1993, pages 110 – 125. Springer-Verlag, 1993. Volume 773/1993 of Lecture Notes in Computer Science.* ***20.*** *M. Bellare, P. Rogaway. Provably Secure Session Key Distribution: The Three Party Case. 27th ACM Symposium on the Theory of Computing - STOC 1995, pages 57– 66. ACM Press, 1995.* ***21****. R. Choo, C. Boyd, Y. Hitchcock. Examining Indistinguishability-Based Proof Models for Key Establishment Protocols, to appear in Advances in Cryptology - Asiacrypt 2005, LNCS 3788, pp.585-604.* ***22.*** *S. Blake-Wilson, D. Johnson, A. Menezes, Key Agreement Protocols and their Security Analysis, the Sixth IMA International Conference on Cryptography and Coding, Cirencester, England, 1997.* ***23.*** *S. Blake-Wilson, A. Menezes, Entity Authentication and Authenticated Key Transport Protocols Employing Asymmetric Techniques, Security Protocols Workshop '97, 1997.* ***24.*** *R. Canetti, H. Krawczyk. Analysis of key-exchange protocols and their use for building secure channels., Advances in Cryptology – Eurocrypt 2001, pages 453 – 474. Springer-Verlag, 2001. http://eprint.iacr.org/2001/040/.* ***25.*** *R. Choo, C. Boyd ,Y. Hitchcock. The Importance of Proofs of Security for Key Establishment Protocols: The Importance of Proofs of Security for Key Establishment Protocols, Information Security Institute, Queensland University of Technology,2005.* ***26.*** *K.-K. R. Choo, C. Boyd, Y. Hitchcock, G. Maitland. On Session Identifiers in Provably Secure Protocols: The Bellare-Rogaway Three-Party Key Distribution Protocol Revisited. In 4th Conference on Security in Communication Networks - SCN 2004, Amalfi, Italy, LNCS 3352/2005 (pp. 352 – 367), 8 – 10 Sep 2004. 27. N. Koblitz, A. Menezes. Another look at "provable security". Cryptology ePrint Archive, Report 2004/152, 2004.* ***28.*** *Y. Hitchcock, Y. Shing Terry Tin, J. M. Gonz'alez Nieto, C. Boyd, P. Montague. A password-based authenticator: Security proof and applications. In Indocrypt 2003, pages 388 – 401. Springer-Verlag, 2003.* ***29.*** *Y. Hitchcock, C. Boyd, J. M. Gonz'alez Nieto. Modular proofs for key exchange: rigorous optimizations in the Canetti–Krawczyk model Springer-Verlag 2005.*