УДК 004.056.55

IND-CPA БЕЗПЕКА МЕХАНІЗМУ ОБ'ЄДНАННЯ КЛЮЧІВ НА ОСНОВІ КОНКАТЕНАЦІЇ

В. В. Балацька[1,a]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У роботі формалізовано сценарій, у якому використання нестійкої функції створення ключа призводить до втрати стійкості механізму об'єднання ключів на основі конкатенації (CtKDF) відносно атаки нерозрізнення з вибраним відкритим текстом (IND-CPA). Запропонована модель із двома іграми: у першій зловмисник отримує значення нестійкої функції створення ключа, у другій — випадкове значення. Здатність зловмисника розрізнити ці два випадки визначає рівень безпеки механізму CtKDF. Проведений аналіз підкреслює важливість безпечної функції створення ключів для забезпечення загальної безпеки гібридних схем.

Ключові слова: функція створення ключів, IND-CPA стійкість, механізм об'єднання ключів на основі конкатенації

Вступ

З поширенням квантових обчислень постає необхідність переходу від класичних криптографічних алгоритмів до постквантових рішень, здатних протистояти квантовим атакам. Одним із перспективних підходів є гібридизація — поєднання традиційних та постквантових алгоритмів у межах одного криптографічного протоколу. Такий підхід дозволяє забезпечити поступовий перехід до нових стандартів без втрати поточної безпеки.

Основним компонентом гібридних схем є механізм об'єднання (combiner), який поєднує вихідні дані, отримані з різних криптографічних схем, для створення спільного секретного значення. Зазвичай, після цього отримане секретне значення додатково обробляється функцією створення ключа для забезпечення необхідних криптографічних властивостей. Проте використання ненадійного механізму об'єднання або слабкої функції створення ключа може зробити всю гібридну конструкцію вразливою до атак, навіть якщо кожен окремий компонент є стійким.

У роботі формалізована модель, у якій слабкість функції створення ключа призводить до порушення стійкості гібридної схеми до атак розрізнення з вибраним відкритим текстом (IND-CPA). Для цього використовується відповідна ігрова модель.

1. Механізм об'єднання з використанням операції конкатенації

Описаний у пункті механізм об'єднання взято з роботи Метью Кампагна «Безпека інкапсуляції гібридних ключів» [1].

Механізм об'єднання з використанням операції конкатенації створює проміжне секретне значення шляхом конкатенації двох або більше спільних секретних значень, що створені різними схемами. Утворений проміжний секрет передається функції створення ключа разом із даними, які отримуються з усієї публічної інформації, виробленої за допомогою функції форматування. Результатом роботи функції створення ключа є спільне секретне значення, що створене гібридною схемою і може використовуватися як ключ.

Алгоритм 1. CtKDF (context, label, l, psk, k, P, R) [1]

$secret \leftarrow psk \| k_1 \| k_2 \| \dots \| k_n$
$context' \leftarrow f(context, P, R)$
return $KDF(secret, label, context', l)$

Незважачи на те, що механізм об'єднання за допомогою операції конкатенації на перший погляд виглядає як ефективний і безпечний підхід для створення спільного секретного значення у гібридних схемах, подальший аналіз показує: його стійкість критично залежить від стійкості використовуваної функції створення ключа. Якщо така функція не є криптографічно стійкою до атак типу IND-CPA, це може знизити рівень захищеності всієї схеми. Відповідно, механізм CtKDF (Алгоритм 1.) сам по собі

[a] viktoriabalatska21@mail.com

не гарантує належного рівня стійкості та може бути вразливим у разі використання нестійкої функції створення ключа.

2. Стійкість функції створення ключа

Означення 1. *[2] Функція створення ключа — функція від чотирьох аргументів (inp, s, c, len), яка створює спільне секретне значення із вхідного значення, де*

- inp *— вхідне значення,*
- s *— сіль,*
- c *— довільна інформація, пов'язана з вихідним секретним значенням,*
- len *— бажана довжина вихідного секретного значення.*

Щоб довести, що гібридна схема CtKDF не є стійкою до IND-CPA атаки, досить розглянути випадок використання нестійкої функції створення ключа. Припустимо, що функція створення ключа повертає те ж саме, що і приймає на вхід.

Алгоритм 2. Гра $G^{\text{kdf-weak}}_{0,\text{KDF},Salt,Input}(\mathscr{A})$ [2]

1: $(inp, a) \leftarrow Input()$
2: **if** $\perp (inp, a)$ **then**
3: **return** 0
4: **end if**
5: $s \leftarrow Salt()$
6: $(c, len) \leftarrow \mathscr{A}(a, s)$
7: $out \leftarrow (inp, s, c, len)$
8: **return** $\mathscr{A}(out)$

Алгоритм 3. Гра $G^{\text{kdf-weak}}_{1,\text{KDF},Salt,Input}(\mathscr{A})$ [2]

1: $(inp, a) \leftarrow Input()$
2: **if** $\perp (inp, a)$ **then**
3: **return** 0
4: **end if**
5: $s \leftarrow Salt()$
6: $(c, len) \leftarrow \mathscr{A}(a, s)$
7: $out \leftarrow \{0,1\}^{len}$ ▷ випадковий рядок довжини len
8: **return** $\mathscr{A}(out)$

Зауваження. *1) У грі G_0 (Алгоритм 2.) зловмисник отримує значення функції створення ключа: $KDF(inp, s, c, len) = out$, де $inp = Input()$ створює початковий матеріал, а $s = Salt()$ додає випадковість.*

2) У грі G_1 (Алгоритм 3.) замість реального значення використовується випадкове значення тієї ж довжини.

Оцінка переваги зловмисника у моделі слабкої функції створення ключа. Нехай маємо функцію створення ключа, Input — джерело вхідного ключового матеріалу, Salt — джерело солі, $\mathscr{A}$ та $\mathscr{A}'$ — пара процедур, що моделюють зловмисника. Тоді перевага зловмисника проти стійкої функції створення ключа, коли вона використовує вхідний матеріал з джерела $Input$ та випадкову сіль $Salt$ для створення ключа, визначається як:

$$\text{Adv}^{\text{kdf-weak}}_{KDF,\text{Input},\text{Salt}}(\mathscr{A}) = \left|\Pr\left[G^{\text{kdf-weak}}_{0,KDF,\text{Input},\text{Salt}}(\mathscr{A}) = 1\right] - \Pr\left[G^{\text{kdf-weak}}_{1,KDF,\text{Input},\text{Salt}}(\mathscr{A}) = 1\right]\right|,$$

де

- $\Pr\left[G^{\text{kdf-weak}}_{0,KDF,Input,\text{Salt}}(\mathscr{A}) = 1\right]$ — ймовірність того, що атака зловмисника на функцію створення ключа буде успішною;
- $\Pr\left[G^{\text{kdf-weak}}_{1,KDF,Input,\text{Salt}}(\mathscr{A}) = 1\right]$ — ймовірність того, що атака зловмисника у випадковому сценарії буде успішною.

Чим ближча ця різниця до нуля, тим менш ймовірно, що зловмисник зможе відрізнити реальний вихід функції створення ключа від випадкового значення, тобто безпечнішою є гібридна схема CtKDF.

Якщо ж ця різниця значна, то зловмисник може легко відрізнити вихід функції створення ключа від випадкового, що свідчить про незахищеність схеми.

Обчислення ймовірності успіху у грі G_0

У цій грі зловмисник бачить реальний вихід функції $\text{KDF}(inp, s, c, len) = out$, де:

- $(inp, a) \leftarrow Input()$ — вхід.
- $s \leftarrow \text{Salt}()$ — сіль.
- $(c, len) \leftarrow \mathscr{A}(a, s)$ — параметри, що вибирає зловмисник.

Тоді:

$$\Pr\left[G^{\text{kdf-weak}}_{0,KDF,Input,\text{Salt}}(\mathscr{A}) = 1\right] = \Pr\left[G_0(\mathscr{A}) = 1\right] = \mathbb{E}_{(inp,a)\leftarrow Input(),\, s\leftarrow\text{Salt}()}\left[\mathbb{I}\left(\mathscr{A}(inp, s, \mathscr{A}(a, s)) = 1\right)\right],$$

де $\mathbb{I}(\cdot)$ — індикаторна функція, яка дорівнює 1, якщо умова виконується.

Обчислення ймовірності успіху у грі G_1

У цій грі вихід функції створення ключа замінюється випадковим рядком:

$$out \leftarrow \{0,1\}^{len}.$$

Ймовірність виграшу зловмисника:

$$\Pr\left[G^{\text{kdf-weak}}_{1,KDF,Input,\text{Salt}}(\mathscr{A}) = 1\right] = \Pr\left[G_1(\mathscr{A}) = 1\right] = \mathbb{E}_{\substack{(inp,a)\leftarrow Input(),\\ s\leftarrow\text{Salt}(),\\ (c,len)\leftarrow\mathscr{A}(a,s)}}\left[\mathbb{E}_{u\leftarrow\{0,1\}^{len}}\left[\mathbb{I}\left(\mathscr{A}(u) = 1\right)\right]\right].$$

Загальна перевага зловмисника

$$\text{Adv}^{\text{kdf-weak}}_{\text{KDF},Input,\text{Salt}}(\mathscr{A}) = \left|\mathbb{E}_{(inp,a),s}\left[\mathbb{I}\left(\mathscr{A}(inp, s, \mathscr{A}(s)) = 1\right)\right] - \mathbb{E}_{(inp,a),s,(c,len)}\left[\mathbb{E}_{u\leftarrow\{0,1\}^{len}}\left[\mathbb{I}(\mathscr{A}(u) = 1)\right]\right]\right|.$$

Побудова стратегії зловмисника $\mathscr{A}$ при використанні нестійкої функції створення ключа

Для подальшої оцінки стійкості побудуємо модель зловмисника $\mathscr{A}$. Метою зловмисника є відрізнити гру G_0 (де він отримує реальне значення функції створення ключа) від гри G_1 (де він отримує випадковий двійковий рядок довжини len).

Стратегія зловмисника $\mathscr{A}$

1. Отримавши значення солі s, зловмисник обчислює:
$$c = 0^{n_c}, \quad len_{out} = |inp| + |s| + |c| + |len|,$$
(далі $|inp| = n_{inp}, |s| = n_s, |c| = n_c, |len| = n_l$) тобто c — це n_c нулів, len_{out} — повна довжина очікуваного виходу, n_{inp}, n_s, n_c, n_l — довжини inp, s, c, l відповідно.
2. Зловмисник надсилає (c, len_{out}) як відповідь на запит.
3. Отримавши значення $out \in \{0,1\}^{len_{out}}$, він ділить його на чотири блоки згідно зі схемою декодування:
$$out = (inp', s', c', len').$$
4. Зловмисник перевіряє, чи:
$$c' = 0^n \quad \text{та} \quad len' = len.$$
5. Якщо умова виконується, він повертає біт 1 (гіпотеза: гра G_0), інакше — 0 (гіпотеза: гра G_1).

З огляду на визначення функції створення ключа, така перевірка завжди проходить успішно.

При використанні такої стратегії зловмисника імовірності матимуть вигляд:

Ймовірність успіху:

$$\Pr\left[G_0(\mathscr{A}) = 1\right] = \\ = \sum_{\substack{inp \in \{0,1\}^{n_{inp}} \\ s \in \{0,1\}^{n_s}}} \Pr[Input() = inp] \cdot \Pr[\text{Salt}() = s] \cdot 1 = 1,$$

бо індикаторна функція $\mathbb{I}$[перевірка пройдена] = 1 для всіх можливих inp, s, оскільки зловмисник точно знає структуру виходу.

2) У грі G_1 вихід out обчислюється випадково як:

$$out \leftarrow \{0,1\}^{len},$$

тобто:

$$out \sim \mathrm{U}(\{0,1\}^{len}),$$

де $U(\{0,1\}^{len})$ — рівномірний розподіл.

Зловмисник намагається перевірити, чи значення out має структуру вигляду (inp, s, c, len), зокрема чи $c = 0^{n_c}$ та len_{out} збігається із закодованим len. Метою є виявлення ознак невипадковості, що дозволяє відрізнити out від випадкового рядка.

$\Pr\left[\text{останні } n_c + n_l \text{ бітів } out = (0^{n_c}, len)\right] = 2^{-(n_c+n_l)}$.

Ймовірність успіху:

$$\Pr\left[G_1(\mathscr{A}) = 1\right] = 2^{-(n_c+n_l)}.$$

Перевага зловмисника $\mathscr{A}$

$$\mathrm{Adv}^{\text{kdf-weak}}_{\mathrm{KDF},Input,\mathrm{Salt}}(\mathscr{A}) = \left|\Pr\left[G_0(\mathscr{A}) = 1\right] - \Pr\left[G_1(\mathscr{A}) = 1\right]\right| = \\ = \left|1 - 2^{-(n_c+n_l)}\right| = 1 - 2^{-(n_c+n_l)}.$$

Це показує, що зловмисник має максимальну перевагу за умов малих n_c, n_l.

3. Модифікація схеми CtKDF у випадку нестійкої функції створення ключа

Оскільки функція створення ключа, що використовується в схемі CtKDF, штучно зроблена нестійкою, її можна виключити з конструкції, спростивши схему до вигляду (Алгоритм 4.):

Алгоритм 4. CtnoKDF(context, label, l, psk, k, P, R)

$secret \leftarrow psk \| k_1 \| k_2 \| \ldots \| k_n$
$context' \leftarrow f(context, P, R)$
return $secret$

Гра IND-CPA для схеми CtKDF

Розглянемо гібридну схему CtKDF без використання функції створення ключа. Нехай $\mathscr{A}$ — зловмисник, що має доступ до оракула інкапсуляції. Формалізуємо гру IND-CPA як взаємодію між зловмисником та чесним гравцем (Challenger):

Гра $\mathbf{IND\text{-}CPA}^{\mathscr{A}}_{\mathbf{CtKDF}}$:

1. **Setup:**
   - Для кожного $i \in \{1, \ldots, n\}$:
   $$(sk[i], pk[i]) \xleftarrow{\$} \mathsf{KGen}_i(),$$
   де sk, pk — особистий та відкритий ключі відповідно.
   - Встановити $pk := (pk[1], \ldots, pk[n])$.
   - Вибрати біт $b \xleftarrow{\$} \{0,1\}$.
   - Передати значення pk зловмиснику $\mathscr{A}$.
2. **Оракул інкапсуляції:**
   - $\mathscr{A}$ може багаторазово викликати оракул інкапсуляції:
   $$(ct, secret) \leftarrow \mathsf{Enc}(pk').$$
   - Для кожного $i \in \{1, \ldots, n\}$:
   $$(k[i], c[i]) \xleftarrow{\$} \mathsf{Enc}_i(pk'[i]).$$
   - Оракул обчислює значення:
   $$secret := k[1] \,\|\, k[2] \,\|\, \ldots \,\|\, k[n],$$
   $$ct = (c[1], \ldots, c[n]).$$
   - Оракул повертає пару $(ct, secret)$ зловмиснику.
3. **Фаза виклику:**
   - $\mathscr{A}$ подає пару відкритих ключів чесному гравцю:
   $$(pk^{(0)}, pk^{(1)}).$$

- Чесний гравець створює пари випадкових ключів та шифротекстів для кожного $pk^{(b)}$:

$$(k_b[i], c_b[i]) \xleftarrow{\$} \mathsf{Enc}_i(pk^{(b)}[i]) \quad \text{для всіх } i.$$

- Обчислити:

$$secret^* := k_b[1] \,\|\, k_b[2] \,\|\, \ldots \,\|\, k_b[n],$$
$$ct^* := (c_b[1], \ldots, c_b[n]).$$

- Повернути $(ct^*, secret^*)$ зловмиснику.

4. **Фаза вгадування:**
   - $\mathscr{A}$ повертає гіпотезу $b' \in \{0,1\}$.
   - Вихід гри: 1 якщо $b' = b$, інакше 0.

Доведення IND-CPA нестійкості гібридної схеми CtKDF

Розглянемо гібридну нововведену схему CtnoKDF. Вона складається з n незалежних схем інкапсуляції ключа та функції створення ключа, введеної вище.

Для доведення IND-CPA нестійкості схеми розглянемо три гри:

- G_0 (Алгоритм 5.) — реальна схема CtKDF,
- CtKDF_a (Алгоритм 6.) — секрет модифіковано: компонент a замінено випадковим,
- G_1 (Алгоритм 7.) — повністю випадкове секретне значення.

Алгоритм 5. Гра $G_0^{\text{ind-cpa}}(\mathscr{A})$

$(pk[1], \ldots, pk[n]) \leftarrow \mathsf{KGen}()$
$b \leftarrow \{0,1\}$
$(pk^{(0)}, pk^{(1)}) \leftarrow \mathscr{A}(pk[1], \ldots, pk[n])$
for $i = 1$ to n **do**
    $(k[i], c[i]) \leftarrow \mathsf{Enc}_i(pk^{(b)}[i])$
end for
$secret \leftarrow k[1] \| \ldots \| k[n]$
$okm \leftarrow \mathsf{KDF}(secret, info, \ell)$
$ct \leftarrow (c[1], \ldots, c[n])$
$b' \leftarrow \mathscr{A}(ct, okm)$ **return** $[b' = b]$

Алгоритм 6. Гра $\mathsf{CtKDF}_a(\mathscr{A}, m)$

$(pk[1], \ldots, pk[n]) \leftarrow \mathsf{KGen}()$
$b \leftarrow \{0,1\}$
$(pk^{(0)}, pk^{(1)}) \leftarrow \mathscr{A}(pk[1], \ldots, pk[n])$
for $i = 1$ to n **do**
    if $i = m$ **then**
        $k[i] \leftarrow \{0,1\}^{\ell}$
        $c[i] \leftarrow \perp$
    else
        $(k[i], c[i]) \leftarrow \mathsf{Enc}_i(pk^{(b)}[i])$
    end if
end for
$secret \leftarrow k[1] \| \ldots \| k[n]$
$okm \leftarrow \mathsf{KDF}(secret, info, \ell)$
$ct \leftarrow (c[1], \ldots, c[n])$
$b' \leftarrow \mathscr{A}(ct, okm)$ **return** $[b' = b]$

Алгоритм 7. Гра $G_1^{\text{ind-cpa}}(\mathscr{A})$

$(pk[1], \ldots, pk[n]) \leftarrow \mathsf{KGen}()$
$b \leftarrow \{0,1\}$
$(pk^{(0)}, pk^{(1)}) \leftarrow \mathscr{A}(pk[1], \ldots, pk[n])$
for $i = 1$ to n **do**
    $(k[i], c[i]) \leftarrow \mathsf{Enc}_i(pk^{(b)}[i])$
end for
$okm \leftarrow \{0,1\}^{\ell}$ ▷ випадкове значення
$ct \leftarrow (c[1], \ldots, c[n])$
$b' \leftarrow \mathscr{A}(ct, okm)$ **return** $[b' = b]$

Теорема 1 (нестійкість гібридної схеми при нестійкій функції створення ключа)**.** *Для будь-якого m ($1 \le m \le n$), тобто для довільної окремої компоненти секрету m та зловмисника $\mathscr{A}$, якщо криптографічна схема є IND-CPA-стійкою, а функція створення ключа не є криптографічно стійкою, тоді має місце така оцінка:*

$$\left|\Pr\left[G_0^{\text{ind-cpa}}(\mathscr{A}) = 1\right] - \Pr\left[\mathsf{CtKDF}_a(\mathscr{A}, m) = 1\right]\right| \ge 1 - \varepsilon_1,$$

де ε_1 — ймовірність успіху IND-CPA атаки на криптографічну схему.

Доведення. Припустимо, що криптографічна схема є IND-CPA-стійкою з імовірністю:

$$\left|\Pr\left[G_0(\mathscr{A}) = 1\right] - \Pr\left[\mathsf{CtKDF}_a(\mathscr{A}, m) = 1\right]\right| \le \varepsilon_1.$$

Це твердження використовується у класичному доведенні стійкості CtKDF. Тут аналізується випадок, коли функція KDF є штучно зроблена нестійкою.

У такому випадку, у грі G_0 зловмисник має доступ до необробленого секретного значення $k_1 \| \ldots \| k_n$, що надає йому значно більше інформації для розрізнення випадку $b = 0$ та $b = 1$, ніж у грі CtKDF_a, де одна компонента замінена на випадкову.

Оскільки ця додаткова інформація не обробляється функцією створення ключа, зловмисник може відрізнити випадок використання G_0 від CtKDF_a з імовірністю принаймні $1 - \varepsilon_1$. □

Теорема 2 (оцінка успіху атаки на нестійку функцію створення ключа)**.** *Для будь-якої компоненти m ($1 \le m \le n$) та будь-якого алгоритму зловмисника $\mathscr{A}$, якщо функція створення ключа не є криптографічно стійкою, тоді:*

$$\left|\Pr\left[\mathsf{CtKDF}_a(\mathscr{A}, m) = 1\right] - \Pr\left[G_1(\mathscr{A}) = 1\right]\right| \ge 1 - \varepsilon_2,$$

де ε_2 — ймовірність успіху атаки на функцію створення ключа, яка визначає ймовірність того, що зловмисник $\mathscr{A}$ не зможе відрізнити вихід функції створення ключа від випадкового значення.

Доведення. У грі CtKDF_a, секрет будується на основі справжніх ключів $k_1, \ldots, k_n$, але одна компонента (під індексом m) замінена на випадкову. У

грі G_1, натомість, функцію створення ключа повністю замінено випадковим значенням тієї ж довжини.

Якщо функція створення ключа є повністю нестійкою, то зловмисник має змогу точно розпізнати, чи отриманий результат походить із виклику функції створення ключа, чи є випадковим рядком, бо структура виходу функції створення ключа є передбачуваною.

Перевага зловмисника $\mathscr{A}$ при такій функції визначається як:

$$\mathrm{Adv}^{\text{kdf-weak}}_{\mathsf{KDF},S^+}(\mathscr{A}) = |\Pr[\mathscr{A} \text{ видає } 1 \mid \text{реальний}] - \Pr[\mathscr{A} \text{ видає } 1 \mid \text{випадковий}]|.$$

У випадку нестійкості функції створення ключа ця перевага досягає $\geq 1 - \varepsilon_2$. Тобто ймовірність, з якою зловмисник може відрізнити ці ігри, є не меншою за $1 - \varepsilon_2$, що й доводить твердження. □

Теорема 3 (зведена теорема про нестійкість схеми CtKDF)**.** *Нехай m $(1 \leq m \leq n)$ та $\mathscr{A}$ — зловмисник у грі IND-CPA для CtKDF. Якщо:*

- *Криптографічна схема є IND-CPA-стійкою з перевагою не більшою за ε_1, тобто*

$$Adv^{\mathsf{ind\text{-}cpa}}_{\text{схема},S_m}(\mathscr{B}) \leq \varepsilon_1,$$

- KDF *не є криптографічно стійкою і*

$$Adv^{\mathsf{kdf\text{-}weak}}_{\mathsf{KDF},S^+}(\mathscr{C}) \geq 1 - \varepsilon_2,$$

тоді CtKDF не є IND-CPA стійкою і виконується оцінка:

$$Adv^{\mathsf{ind\text{-}cpa}}_{\mathsf{CtKDF}}(\mathscr{A}) \geq 1 - (\varepsilon_1 + \varepsilon_2).$$

Доведення. Маємо наступну послідовність переходів між іграми:

$$\begin{aligned}\mathrm{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{CtKDF}}(\mathscr{A}) &= \left|\Pr[G_0(\mathscr{A}) = 1] - \Pr[G_1(\mathscr{A}) = 1]\right| = \\ &= \left|\Pr[G_0(\mathscr{A}) = 1] - \Pr[\mathsf{CtKDF}_a(\mathscr{A}, m) = 1]\right| + \\ &+ \left|\Pr[\mathsf{CtKDF}_a(\mathscr{A}, m) = 1] - \Pr[G_1(\mathscr{A}) = 1]\right|.\end{aligned}$$

З теореми 1 випливає, що:

$$\left|\Pr[G_0(\mathscr{A}) = 1] - \Pr[\mathsf{CtKDF}_a(\mathscr{A}, m) = 1]\right| \geq 1 - \varepsilon_1.$$

З теореми 2 випливає, що:

$$\left|\Pr[\mathsf{CtKDF}_a(\mathscr{A}, m) = 1] - \Pr[G_1(\mathscr{A}) = 1]\right| \geq 1 - \varepsilon_2.$$

Звідси маємо:

$$\mathrm{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{CtKDF}}(\mathscr{A}) \geq 2 - (\varepsilon_1 + \varepsilon_2) - 1 = 1 - (\varepsilon_1 + \varepsilon_2),$$

що завершує доведення. □

Перевага зловмисника

$$\mathrm{Adv}^{\text{ind-cpa}}_{\text{CtKDF}}(\mathscr{A}) = \left|\Pr[b' = b] - \frac{1}{2}\right| \geq 1 - (\varepsilon_1 + \varepsilon_2).$$

Цей вираз визначає перевагу зловмисника в атаці розрізнення з вибраним відкритим текстом (IND-CPA). Вона показує, наскільки ймовірність правильного вгадування біта b зловмисником $\mathscr{A}$ перевищує випадкове вгадування. Значення близьке до 1 означає, що зловмисник може з великою ймовірністю розрізнити зашифровані повідомлення, що свідчить про втрату IND-CPA стійкості конструкції.

Формальне твердження

Нехай функція створення ключа не є криптографічно стійкою, тоді перевага зловмисника $\mathscr{C}$ визначається:

$$\mathrm{Adv}^{\text{kdf-weak}}_{\text{KDF},Input^+}(\mathscr{C}) \geq 1 - \varepsilon_2$$

та перевага зловмисника $\mathscr{B}$ у грі визначається як:

$$\mathrm{Adv}^{\text{ind-cpa}}_{\text{схема},Input_m}(\mathscr{B}) \leq \varepsilon_1.$$

Тоді існує зловмисник $\mathscr{A}$, такий, що його перевага у грі проти гібридної схеми CtKDF:

$$\mathrm{Adv}^{\text{ind-cpa}}_{\text{CtKDF}}(\mathscr{A}) \geq 1 - (\varepsilon_1 + \varepsilon_2).$$

Висновки

У роботі проаналізовано стійкість гібридної схеми CtKDF. Доведено, що навіть при IND-CPA-стійких схемах, використання нестійкої функції створення ключа призводить до загальної нестійкості схеми CtKDF. Доведення виконано методом переходів між іграми що підтверджує, що CtKDF не забезпечує IND-CPA-стійкість у випадку нестійкої функції створення ключа.

Отримані результати можуть бути корисними при виборі функції створення ключа у практичному проєктуванні гібридних постквантових протоколів.

Перелік використаних джерел

1. *Campagna M.* Security of Hybrid Key Establishment. — Springer International Publishing, 01.01.2020. — URL: https://www.amazon.science/publications/security-of-hybrid-key-encapsulation.
2. *Campagna M.* Security of Hybrid Key Establishment Using Concatenation. — Springer International Publishing, 01.01.2020. — URL: https://www.amazon.science/publications/security-of-hybrid-key-establishment-using-concatenation.