УДК 004.056.55

doi.org/10.15407/fmmit2023.36.137

Проблеми побудови аксіоматики сучасної криптографії: інформаційний, обчислювальний та інформаційно-обчислювальний підходи

Антон Кудін[1], Володимир Ткач[2], Світлана Носок[3]

[1] д. т. н., с.н.с., Фізико-технічний інститут НТУУ «Київський політехнічний інститут імені Ігоря Сікорського», Берестейський проспект, 37, 030056, Київ, e-mail: pplayshner@gmail.com
[2] к. е. н., Blekinge Institute of Technology (Карлскруна, Швеція) та Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» (Київ, Україна), e-mail: vntkach@gmail.com
[3] к. т. н., доцент, Фізико-технічний інститут НТУУ «Київський політехнічний інститут імені Ігоря Сікорського», Берестейський проспект, 37, 030056, Київ, e-mail: nosok@gmail.com

У роботі наведений аналіз існуючих підходів до побудови аксіоматики криптографічних перетворень, як з точки зору теоретико-інформаційного, так і теоретико-обчислювального підходів до стійкості криптосистем. Показано, що існуючі вади підходів можуть бути вирішені за рахунок об'єднання цих підходів на основі застосування положень загальної теорії оптимальних алгоритмів. Наведені основні криптографічні примітиви та примітивні криптографічні протоколи, побудовані на запропонованому інформаційно-обчислювальному підході.

Ключові слова: криптографічний примітив, примітивний криптографічний протокол,

Вступ. Аксіоматичний або «доказовий» підхід («підхід доведеної стійкості») в криптології реалізується зведенням стійкості новоутворених криптографічних алгоритмів та протоколів до стійкості відомих криптографічних примітивів і протоколів або складності вирішення певних обчислювальних задач, складність яких добре вивчена. При цьому стійкість криптографічного примітиву приймається як аксіома – без доведення. Стаття поділена на три частини: в першій аналізуються результати Шенона щодо побудови алгебри елементарних шифрів [1] практично у відриві від аналізу стійкості отриманих шифрів та започаткування основ загального підходу до обґрунтування стійкості шифрів гамування; в другій – проектування ідей Шенона на сучасний (з точки зору теорії складності алгоритмів) підхід [2] до обґрунтування стійкості криптосистем та складності побудови криптографічних примітивів і аксіоматики на його базі; в третій – нова ідеологія побудови криптографічних примітивів на основі інформаційно-невизначених односторонніх функцій [3], яка розвивається авторами.

1.Алгебра шифрів Шенона та її сучасні модифікації

Нехай M – відкрите повідомлення, K – ключ, E – зашифроване повідомлення, T_i – відображення $M \to E$, індекс i визначається ключем. Тоді шифрування за

Шеноном [1] визначається як однопараметрична родина відображень $E = T_i M$, розшифрування – відповідно за допомогою родини зворотних відображень $M = T_i^{-1} E$, відображення T_i повинно мати єдине зворотне відображення T_i^{-1}, так що $T_i \cdot T_i^{-1} = I$, де I – тотожне відображення. Шенон будує алгебру на основі двох операцій – «добутку шифрів»: $T_j = T_i \cdot T_k$ та «зваженої суми шифрів»: $T_j = pT_i + qT_k$, де $p + q = 1$. Додатковою вимогою, яка суттєво спрощує розгляд побудови аксіоматики в рамках цієї теорії, є введення поняття «чистого шифру». Це такий шифр, в якому для будь яких відображень T_i, T_j, T_k їх добуток $T_i \cdot T_j^{-1} \cdot T_k$ належить цій родині відображень, а ключі з множини ключів (які визначають індекси відображень), обираються з рівною ймовірністю. Введення такого поняття дозволяє показати, що елементарні шифри відносно введених вище операцій добутку (возведення в ступінь) та зваженої суми шифрів утворюють алгебру.

Проблемами аксіоматики Шенона є: встановлюється тільки співвідношення між елементарними класичними шифрами, самі шифри представлені як бінарні відносини між множинами відкритих повідомлень та криптограм (модель, яка дозволяє описувати тільки нескладні класичні симетричні шифри), нечітке введення зв'язку між інформацією та перетворенням, додавання до цих двох примітивів перемішування, яке руйнує доказовий підхід – шифри типу $T_j = S \cdot F \cdot T$, припущення про стійкість шифрів розглядаються на якісному рівні. Це унеможливлює побудову несуперечній аксіоматики з точки зору доведення стійкості криптографічних систем. Оцінки стійкості та побудова практично стійких шифрів в роботі Шенона стоїть осторонь від алгебри шифрів.

2. Аксіоматика на важкооборотних функціях

Після того, як спроба Шенона побудувати аксіоматику криптографії виключно на визначенні співвідношень на множинах відкритих текстів фактично зазнали невдачі, дослідження поділились на два напрямки: перший, пов'язаний з розвитком досконало і ідеально стійких шифрів – у напрямку послаблення вимог до генератора випадкової гами $G: \{0,1\}^k \to \{0,1\}^\infty$ [2-4] та другий, який намагався формалізувати поняття «криптографічне перетворення» за допомогою теорії складності алгоритмів [2]. На другому шляху відразу постали дві проблеми: на відміну від класичного визначення складності алгоритму, як максимальної кількості кроків на множині вхідних даних, потрібно було розглядати модифікацію визначення, як середню кількість кроків для всіх вхідних даних, або навіть так звану «складність практично всюди» [2] та складність зведення практичних шифрів (і криптосистем, криптопротоколів на їх основі) до базових односторонніх функцій «складність» обернення яких приймалась за аксіому. Іншим викликом постала проблема формалізації стійкості асиметричних криптосистем, яка базувалась на уточненні поняття важкооборотних функцій – важкооборотних функцій «з лазівкою» та зв'язку між інформаційною невизначеністю відкритого тексту та шифртексту і обчислювальною складністю обернення функції при відомості одного з ключів шифрування/розшифрування.

За першим напрямком вдалось отримати достатньо вагомі результати. Нехай [4] $\Sigma_в = (X, Y, K, E_k, D_k, P(X), P(K))$ – ймовірнісна модель шифру, для якій $|X| = |Y| = |K|$ (рівність потужності множин відкритих текстів, шифртекстів та ключів відповідно), пасивні атаки криптоаналітика – це відношення на множині $\alpha_p \subseteq X \times Y$, μ – зовнішня міра на множині Y, $\upsilon(x)$ – міра однозначності, як відображення Y в множину зовнішніх мір на X. Тоді шифр є досконало стійким в моделі Шенона тоді і тільки тоді, якщо $|K(x,y)|=1$, для будь-яких $x \in X, y \in Y$ та $p(k) = 1/|K|$ для будь якого ключа $k \in K$, перша міра характеризує потенційну можливість отримання доступу до повідомлень, друга характеризує «ідеальну стійкість», як можливість отримання певної інформації, недостатньої для відновлення повідомлення. Для виміру стійкості використовується щільність множин $\alpha_p(x)$ (в ймовірнісному та обчислювальному сенсі) для кожного x або трійка $(\alpha_p, \mu, \upsilon)$. Ці міри можна змінювати відповідно до моделей – загальної теорії множин (класичний випадок Шенона), ймовірнісної, інформаційної, теорії складності обчислень, алгоритмічної теорії інформації. За даним підходом доведено [4] недосконаліть стійкості шифру Вернама при відсутності слабих ключів, а також те, що результат операції $\oplus$, застосованої до випадкової та невипадкової послідовності може бути не випадковою, ні навіть псевдовипадковою послідовністю. Це закриває можливість побудови аксіоматики криптоперетворень виключно шляхом побудови ідеального генератора гами в теоретичному сенсі. До того, існують чисто практичні складності побудови як ідеального генератора гами, так і оцінки його якості і в практичному сенсі. Маємо [5] справедливе твердження: «Існує ансамбль джерел повідомлень X_n із ефективною ентропією $H_c(X_n)$ набагато більшою, ніж класична ентропія $H(X_n)$. Для будь-якої функції $g(n)$, такої, що $(\log_2 n)^2 < g(n) < n$ існує ансамбль джерел повідомлень, такий, що $H(X_n) = g(n), H_c(X_n) = n + O(n^{-t})$ ». Неможливість оцінки кількості інформації за рахунок складності кодування відкритих повідомлень X також демонструє справедливість наступної теореми: «Нехай $f(n)$ – така функція, що $f(n) = o(n)$ та $f(n) \geq \log n$, та x_n - така послідовність, що $K(x_n) = n + O(f(n))$. Тоді існує послідовність y_n, така, що $K(y_n) = n + O(f(n)), I(x_n : y_n) = a \cdot n + O(f(n))$, для будь-яких $0 < a < 1$ та для будь-якої послідовності слів z_n, які задовольняють умові $K(z_n \mid x_n) = O(f(n)), K(z_n \mid y_n) = O(f(n))$, тоді виконано $K(z_n) = O(f(n))$.»
Розгляд другого шляху привів до появи нової теорії обчислювальної складності «майже для всіх вхідних даних» [2,3] та досліджень алгебраїчної природи односторонніх криптографічних перетворень (стійкість «в поліноміальному сенсі», «шифри, що не зберігають будь-які гомоморфізм» та інші [2,3]). Проте, всі ці дослідження не відповідали на питання побудови елементарних

перетворень, стійкість яких приймаємо за аксіому і шляхів строгого зведення шифрів, що застосовуються до таких елементарних перетворень. Першім цікавим випадком є побудова штучних обчислювальних моделей, для яких будь-який алгоритм криптоаналізу належав би виключно до класу NP. Другим – розвиток цієї ідеї, що лягло в концепцію ймовірнісного шифрування [2]. За рахунок введення аксіом про стійкіть до криптоаналізу ідеальних генераторів випадкових послідовностей $G:\{0,1\}^k \to \{0,1\}^\infty$ та геш-функцій $H:\{0,1\}^\infty \to \{0,1\}^k$ вдалось довести наступне твердження [2]: «Нехай A – поліноміальна ймовірнісна машина Тьюринга, що моделює дії криптоаналітика; G – алгоритм генерації ключів, E,D – алгоритми шифрування/розшифрування, X – множина відкритих текстів, Y – множина шифртекстів, Q – довільний поліном, тоді існує криптосистема (G,E,D,X,Y) така що, будь-яка A визначає X при відомих E,Y з ймовірністю не більше, ніж $1/2 + 1/Q(k)$, где k – обраний параметр стійкості до криптоаналізу». Третім (найбільш вдалим) випадком є використання як одного криптографічного примітива, стійкість якого маємо за аксіому, неінтерактивного протоколу доказу із нульовими знаннями [6]. В основі практичних конструкцій на базі цього підходу лежать концепції випадкового оракула [2,7], еталонного загального рядку та узагальненої моделі еталонного загального рядку [8]. Відомо, що існує відображення із множини протоколів із оракулом у множину протоколів без оракула, але тоді окремі протоколи узгодження ключів не можуть бути реалізовані в моделі випадкового оракула. Аналогічно стверджується, що і для протоколів електронного цифрового підпису і шифрування, стійких в моделі випадкового оракула, не існує стійкої конкретної реалізації (тобто функції, яка б реалізувала випадковий оракул). Тобто під час конкретної реалізації можливі ситуації (нехай і малоймовірні), коли, наприклад, над повідомленням виконають тотожне перетворення, чи викриється секретний ключ. Відомі також аналогічні вади та складнощі практичної реалізації моделей еталонного загального рядку та узагальненої моделі еталонного загального рядку [8]. Особливістю неінтерактивних систем із нульовим розголошенням є те, що вони завжди мають інтегруватись в конструкцію конкретного прикладного криптоалгоритму чи протоколу. Таких як наприклад обчислення у білінійних групах, асиметричні схеми шифрування, стійкі до атак на вибраний закритий текст. Доводиться стверджувати [8], що є доведення можливості існування такого протоколу, проте його конкретна надійна реалізація на сьогодні - невирішена у загальному випадку задача.

3. Поєднання підходів – аксіоматика на основі інформаційно-обчислювального підходу або криптографічні примітиви на основі нечітких та неповних інформаційних операторах

Односторонні функції побудовані при умові, що інформація для обчислення задана повно та точно. Узагальненням є ситуація, коли інформація для функції задається непрямо, а за допомогою інформаційного оператора, який може бути неповним та неточним [5]. Введемо наступні позначення. Нехай задані множини

X, Y. Нехай 2^Y - клас усіх підмножин множини Y. Розглянемо оператор $S: X \times \Re_+ \to 2^Y$, де $\Re_+ = [0, \infty)$, так званий оператор рішення, який має такі властивості: $S(x,0) \neq \varnothing, \forall x \in X$, $\delta_1 \leq \delta_2 \Rightarrow S(x, \delta_1) \subset S(x, \delta_2)$, $\forall \delta_1, \delta_2 \in \Re_+, x \in X$. Для заданого $\varepsilon \geq 0$ елемент $y \in Y$, який задовольняє умові $y \in S(x, \varepsilon)$ назвемо ε – наближенням. Задача пошуку ε – наближення розглядається при умові відсутності повної та точної інформації про x, але відомо $N(x)$, де: $N: X \to Y$ – інформаційний оператор, а Y - образ множини X. За відомим $N(x)$ потрібно знайти ε – наближення до x. Якщо множина $V(N, x) = \{\tilde{x} \in X : N(\tilde{x}) = N(x)$ всіх елементів $\tilde{x}$, які є нерозрізненими за допомогою $N(x)$ містить один елемент, то оператор N встановлює функціональну залежність між множинами X, Y та зветься повним. Оператор рішення, який застосовується до неповного інформаційного оператора, породжує множину $A(N, f, \varepsilon) = \bigcap_{\tilde{x} \in V(N,x)} S(\tilde{x}, \varepsilon)$, при цьому для $\delta_1 \leq \delta_2 \Rightarrow A(N, x, \delta_1) \subset A(N, x, \delta_2)$. Тоді $r(N, x) = \inf\{\delta : A(N, x, \delta) \neq \varnothing\}$ та $r(N) = \sup_{x \in X} r(N, x) (= \inf\{\delta : A(N, x, \delta) \neq \varnothing, \forall x \in X\})$ визначають ніжні оцінки точності рішень, які можуть бути досягнуті при умові неповного інформаційного оператора. На множині ідеальних алгоритмів $\Phi(N) : N(x) \to G$, із визначеними локальною $e(\phi, N, x) = \inf\{\delta : \phi(N(x)) \in A(N, x, \delta)\}$ та глобальною $e(\phi, N) = \sup_{x \in X} \varepsilon(\phi, N, x)$ похибками інформація $N(x)$ дозволяє знаходити ε - наближення для будь-якого $x \in X$ тоді і тільки тоді, якщо виконується одна з умов: $r(N) < \varepsilon$, $r(N) = \varepsilon, \exists \phi : \phi(N(x)) \in S(x, e(\phi, N)), \forall x \in X$. У випадку наближеної інформації N_ρ (ρ – міра похибки) результати для нижніх оцінок визначаються аналогично: $r(N_\rho) < \varepsilon$, $r(N_\rho) = \varepsilon, \exists \phi : \phi(N_\rho(x)) \in S(x, e(\phi, N_\rho)), \forall x \in X$. На відміну від точного інформаційного оператора, оператор N_ρ визначається через оператор інформаційної помилки $E: H \times \Re_+ \to 2^H$, який має властивості: $E(h, 0) \neq \varnothing, \forall h \in H$, $\delta_1 \leq \delta_2 \Rightarrow E(h, \delta_1) \subset S(h, \delta_2)$, $\forall \delta_1, \delta_2 \in \Re_+, h \in H$. Наближений оператор $N_\rho : X \to H$ задовольняє умові: $N_\rho(x) \in E(N(x), \rho), \forall x \in X$. Зауважимо, що якщо точний інформаційний оператор N є неповним, то N_ρ також є неповним, якщо ж N є повним, то N_ρ може бути як повним, так і неповним. Якщо оператор N_ρ є повним, то $r(N_\rho) = 0$. Визначимо X – множина відкритих текстів, тоді $N: X \to Y$ – оператор, який відображає криптографічне перетворення, $S: X \times \Re_+ \to 2^G$ оператор криптографічного анализу, G – множина критеріїв належності до множини X. Як $\Phi(N(X))$ обираємо множину ідеальних алгоритмів ϕ реализації оператора криптоанализу. При цьому умова ідеальної стійкості визначається як $r(N(X)) \geq \varepsilon > 0$, де $r(N(X))$ - радіус

інформації $N(X)$. Визначимо введену модель стійкості як «модель ЗТОА». Справедливі наступні теореми. «Для криптосистем, ідеально стійких в моделі ЗТОА, усі криптографічні перетворення мають властивість не зберігати гомоморфизм». З неї витикає теорема «Криптосистема, ідеально стійка в моделі ЗТОА, також є стійкою в сенсі поліноміальної нерозрізненості».

Висновки. Аксіоматика криптосистем на основі інформаційно-обчислювального підходу є узагальненням аксіоматики на базі чисто інформаційного або чисто обчислювального (поліноміальної нерозрізненості, збереження гомоморфізму та анонімності відкритих ключів) підходів. Інформаційно невизначені односпрямовані функції є достатньо адекватними реальним конструкціям моделями, де навіть наявність у порушника навіть обраної пари «криптограма/відкритий текст» не дає повної інформації про обраний відкритий ключ, оскільки рандомізація вноситься в зв'язок відкритого та особистого ключа. За загальний вимір стійкості криптосистем при такому підході можна обрати радіус інформації.

Література

[1] *К. Шеннон* Теория связи в секретных системах / в кн. К. Шеннон «Работы по теории информации и кибернетике», М., ИЛ, 1963, с. 333-369.
[2] *Goldreich O.* Foundations of Cryptography. Volume 1. Basic Tools. – London: Cambridge University Press, 2001. – 555 p.
[3] *В.К. Задирака, А.М. Кудин* Новые модели и методы определения стойкости систем защиты информации / Кибернетика и системный анализ. – 2017. – Том 53. - № 6. – С.176-184.
[4] *H. Jurgensen, L. Robbins* Towards foundatioms of cryptography: investigation of perfect secrecy / Journal of universal computer science. – V.2. - № 5. – 1996. – P.347-379.
[5] *A.C. Yao* Theory and application of trapdoor functions / 23rd Annual symposium on foundations of computer science, Chicago, 1982. – P. 80-91.
[6] *M. Blum, A. de Santis, S. Micali, G. Persiano* Non-interactive zero knowledge / SIAM J. COMPUT. Vol. 20, No. 6, pp. 1084-1118, December 1991.
[7] *Bellare Mihir, Rogaway Phillip* Random Oracles are Practical: A Paradigm for Designing Efficient Protocols (англ.) // ACM Conference on Computer and Communications Security : journal. — 1993. — P. 62—73.
[8] *Morais, E., Koens, T., van Wijk, C. et al.* A survey on zero knowledge range proofs and applications. SN Appl. Sci. 1, 946 (2019). https://doi.org/10.1007/s42452-019-0989-z

The problem of modern cryptography axiomatic: information, computational and information-computational approaches

Anton Kudin, Volodimir Tkach, Svetlana Nosok

The paper is considered the issue existing approaches to build the axiomatic of cryptographic transformations. Both point of view (information-theoretic and computational-theoretic) is going through. It is shown that the existing defects of the approaches can be solved by combining these approaches based on the application of the provisions of the general theory of optimal algorithms. The main cryptographic primitives and primitive cryptographic protocols built on the proposed information and computing approach are given.

Отримано 10.04.23