УДК 681.3

А.М. Кудін

ПОРІВНЯЛЬНИЙ АНАЛІЗ МАТЕМАТИЧНИХ МОДЕЛЕЙ СТІЙКОСТІ КРИПТОСИСТЕМ

Вступ

Відомою проблемою криптології є отримання нетривіальних нижніх оцінок стійкості криптосистем, які використовуються на практиці. Незважаючи на численні дослідження в даній галузі [1–5], на сьогодні в загальному випадку задача є не розв'язаною навіть для найпростішого (для криптографії) випадку – аналізу стійкості за умови наявності тільки шифртексту і апріорної інформації про джерело відкритого тексту. Як наслідок – для всіх криптосистем, які використовуються на практиці, застосовується так званий емпіричний метод (метод експертних оцінок, або ad-hoc). За ним стійкість криптосистеми оцінюється відносно *відомих* криптоаналітичних атак або при виконанні певних вимог до перетворень, які пов'язують відкритий текст і шифртекст та ключі шифрування/розшифрування. Публікації останніх років [5, 6] виділяють два напрямки розвитку досліджень у галузі стійкості криптосистем: розробку та дослідження ідеальних моделей криптосистем або дослідження для окремих випадків стійкості криптосистем, які використовуються практично.

Постановка задачі

У даній статті аналізуються моделі криптосистем з точки зору розв'язання задачі наближення теоретичних моделей до реальних криптосистем, а також дослідження та виявлення загальних вимог, які повинна задовольняти "стійка" криптосистема.

Підходи до оцінки стійкості криптосистем

Відомо [7], що існують три загальних підходи до оцінки стійкості криптосистем: теоретико-інформаційний (не існує алгоритму розв'язку задачі криптоаналізу в будь-якої моделі обчислень через відсутність достатньої кількості інформації (вхідних даних)), теоретико-складностний (не існує алгоритму розв'язку задачі криптоаналізу в певній моделі обчислень) та теоретико-системний (фіксується певна множина алгоритмів криптоаналізу, до яких криптосистема є стійкою). Практично до цих трьох підходів додається четвертий – метод експертних оцінок стійкості криптосистеми. Очевидно, що отримання нижніх оцінок стійкості криптосистеми доцільно проводити в рамках об'єднання теоретико-інформаційного та теоретико-складностного підходів, поступово підвищуючи вимоги до моделі обчислень та інформації, доступної для криптоаналітика.

Метою даної статті є аналіз математичних моделей стійкості криптосистем з точки зору необхідної кількості інформації для криптоаналізу при атаці порушення конфіденційності інформації на основі наявного шифртексту (з відомою моделлю джерела відкритого тексту). Для асиметричних криптосистем проаналізуємо взаємозалежність відношення, яке пов'язує ключі шифрування і розшифрування, та відношення, яке пов'язує шифртекст та відкритий текст. Без втрати загальності замість криптосистеми будемо розглядати криптографічне перетворення разом із системою управління ключами.

Нехай (G, K, E, D) – узагальнена алгебрична модель шифру [1], де E – ймовірнісний алгоритм зашифрування, D – ймовірнісний алгоритм розшифрування, множина відкритих повідомлень $X = \{x \mid x = D_{sk}(E_{pk}(x))\}$. На відміну від традиційної алгебричної моделі (X, K, Y, E, D) шифру [8] як сукупності множин відкритого тексту, ключів, шифртексту та відображень шифрування/розшифрування, в узагальненій алгебричній моделі шифр є сукупністю ймовірнісних алгоритмів, а до алгоритму генерації ключа K додається так званий алгоритм генерації загального ключа G, який є узагальненням традиційного рандомізатора, а саме $I \leftarrow G(K), k \in \aleph, (pk, sk) \leftarrow K(I)$, де k – деякий невідомий параметр; (pk, sk) – ключі шифрування та розшифрування. Множина Y визначається як $Y = \{y \mid y = E_{pk}(x)\}$. Стійкість криптосистеми в даному випадку визначається як неможливість отримання $x \in X$ і sk для всіх (або більшості) k деякою множиною $A(pk, E_{pk}(X))$ алгоритмів у моделі обчислень U. Як правило, існування таких алгоритмів залежить від співвідношень, визначених на $X \times Y, X \times K$, структури множини Y та властивостей G, K.

Різні математичні моделі акцентують увагу, як правило, на окремі характеристики зазначених алгебричних структур на основі введених формальних вимірювань, наприклад розподілу ймовірностей. Нашою задачею є пошук універсального показника, зміна значення якого приводила б до рівності $A(pk, E_{pk}(X)) = \varnothing$ для визначеної (достатньо реальної) моделі обчислень U.

Математичні моделі теоретико-інформаційного підходу до стікості криптосистеми

Модель Юргенсона, Роббінса **[2]**. Розглядається загальна ймовірнісна модель шифру $\Sigma_{й} = (X, Y, K, E_k, D_k, P(X), P(K))$. Відомо, що якщо $\Sigma_{й}$ – ймовірнісна модель шифру, для якої $|X| = |Y| = |K|$, то шифр є досконало стійким у моделі Шеннона 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 $k \in K$. Для визначення стійкості в цій моделі вводиться поняття пасивних атак порушника як відношення на множині $\alpha_p \subseteq X \times Y$. На множині Y вводиться зовнішня міра μ. Додатково вводиться так звана міра одиничності $\upsilon(x)$ як відображення Y в множину зовнішніх мір на X. Перша міра характеризує потенційну можливість отримання доступу до повідомлень (на кшталт теоретико-інформаційної стійкості), друга – якщо до деяких повідомлень і можна отримати хоч якусь інформацію, але її недостатньо (як для ідеально стійких криптосистем). Практично як вимір стійкості використовується щільність множин $\alpha_p(x)$ для кожного x. На практиці – це дуже оптимістично, якщо використовувати тільки її. Додатково розглядається щільність $\alpha_p(x)$ в ймовірнісному та обчислювальному аспектах. Потім визначення цих мір уточнюються із врахуванням неоднорідності розподілу повідомлень на множині X. Висуваються гіпотези про недостатність застосування для оцінки стійкості криптосистеми тільки ймовірнісної міри, замість цього розглядається можливість застосування теорії аналізу ризику. Як більш точна модель пасивного порушника використовується трійка $(\alpha_p, \mu, \upsilon)$. При цьому μ – деяка зовнішня міра на множині Y. Ці міри змінюються відповідно до моделей – загальної, ймовірнісної, інформаційної, теорії складності обчислень, алгоритмічної теорії інформації. Показано, що шифр одноразового блокнота, в якому відсутні слабкі ключі, не є досконалим у строгому розумінні в жодній із цих моделей. Цікавим фактом є також те, що якщо випадкові послідовності вводяться в моделі алгоритмічної складності, то сума за модулем 2 випадкової та невипадкової послідовностей може бути ні невипадковою, ні навіть псевдовипадковою послідовністю.

Модель Штарькова сумісної стійкості інформації та ключа в секретних системах **[3]**. Застосовується класична ймовірнісна модель шифру $\Sigma_{й} = (X, Y, K, E_k, D_k, P(X), P(K))$ [8] з додаванням рандомізатора $R(X)$. У рамках цієї моделі як вимір стійкості використовується умовна ентропія $H(X^n | Y^n)$ на ансамблі з n повідомлень. Доводиться, що адаптивна залежність рандомізації від ключа не збільшує загальну стійкість системи. У рамках моделі наводяться приклади як зменшення, так і *збільшення невизначеності* відкритого тексту при спостереженні n криптограм (при $n > 1$). Розглядається залежність невизначеності від розподілу ключів. Доводиться, що рівномірний розподіл ключів не є найкращим для невизначеності.

Моделі алгоритмічної складності множини X **[9, 10]**. Застосовується класична ймовірнісна модель шифру $\Sigma_{й} = (X, Y, K, E_k, D_k, P(X), P(K))$. Додатково до неї досліджується складність кодування слів кінцевої довжини $x_n \in X$. Історично першою з даних моделей є модель Яо [9]. У рамках моделі доводиться твердження: "Існує ансамбль джерел повідомлень X_n з 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 такий ансамбль джерел повідомлень, що $H(X_n) = g(n)$, $H_c(X_n) = n + O(n^{-t})$".

Більш точні оцінки неможливості криптоаналізу за рахунок складності кодування відкритих повідомлень X можна побудувати з використанням моделі алгоритмічної кількості інформації, запропонованої Колмогоровим [10]. Справедлива така теорема [10].

Теорема. Нехай $f(n)$ – така функція, що $f(n) = o(n)$ і $f(n) \geq \log n$, та x_n – така послідовність, що $K(x_n) = n + O(f(n))$. Тоді існує послі-

довність 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 умову $K(z_n | x_n) = O(f(n))$, $K(z_n | y_n) = O(f(n))$. Тоді виконується рівність $K(z_n) = O(f(n))$.

Зауважимо, що ці моделі є першими, які поєднують теоретико-інформаційний та теоретико-складностний підходи до стійкості криптосистем.

Модель анонімності ключа **[1]**. Ці моделі досліджують нову вимогу до стійкості асиметричних криптосистем. Замість традиційної моделі асиметричної криптосистеми (G, K, E, D) вводиться модель $(G, I, K(I), E, D)$, де I – деякий загальний ключ. За наявною криптограмою порушник, який прослуховує обмін інформацією, не в змозі визначити конкретний відкритий ключ (з множини відомих відкритих ключів), за допомогою якого вироблена криптограма. За міру стійкості вибирається так звана перевага супротивника $Adv = P_1 - P_2$ як різниця між ймовірностями розрізнення криптограм від різних відкритих ключів. Це також означає анонімність отримувача інформації перед порушником. Висуваються твердження, що *існуюча* схема Ел-Гамала забезпечує анонімність навіть "з вибраним відкритим текстом" при умові складності проблеми Діффі–Хелмана, схема Крамара–Шоупа – "з вибраним шифртекстом" з тією ж умовою, RSA-перетворення умови анонімності не забезпечує. Пропонується модифікація RSA-OAEP, що забезпечує анонімність та метод побудови односторонньої перестановки з "лазівкою", яка забезпечує анонімність. Згідно з визначенням анонімності в цій моделі всі гетерогенні асиметричні криптосистеми не є анонімними: наприклад, не є анонімною RSA з різними довжинами ключів, тобто не повною має бути інформація про саму криптосистему, яку використовує конкретний абонент (або, наприклад, всі розділяють загальний відкритий параметр). Оскільки деякі схеми задовольняють це визначення стійкості, деякі – ні, авторами моделі пропонується провести дослідження існуючих схем на анонімність. У рамках цієї моделі RSA є менш стійкою порівняно із системами, заснованими на дискретному логарифмі, а властивості прихованості відкритого тексту та прихованості ключа є ортогональними.

Non-malleability (негнучкість, непластичність, нееластичність, незбереження гомоморфізму) **[4]**. Визначається на множині шифртекстів Y таким чином: $\forall y_1, y_2 \in Y$ відносно функції f, визначеної на множині відкритих текстів, не існує ймовірнісного алгоритму поліноміальної складності визначення y_2 за відомим y_1, такого, що $y_1 = E(x_1), y_2 = E(f(x_1))$. Таким чином, криптографічне перетворення "порушує" деяке відношення, визначене на множині відкритих текстів.

Indistinguishability (semantic security) – семантична стійкість, поліноміальна нерозрізненість **[5]**.

Наявність відкритого ключа не дає можливості визначати відповідність множин відкритих текстів і криптограм поліноміальним алгоритмом з імовірністю краще, ніж при випадковому виборі. Позначимо A, M як поліноміальні імовірнісні машини Тьюринга, що характеризують обчислювальні можливості криптоаналітика при наявності інформації про відкритий ключ та шифртекст і без нього, відповідно, G – алгоритм генерації ключів, E, D – відповідно алгоритми шифрування/розшифрування, X – множина відкритих текстів, Y – множина шифртекстів, Q – довільний поліном. Тоді криптосистема (G, E, D) називається стійкою в розумінні поліноміальної нерозрізненості, якщо:

$$P(A(1^k, e, x_0, x_1, c) = x \,|\, (e, d) \leftarrow G(1^k);$$

$$\{x_0, x_1\} \leftarrow M(1^k);\ x \leftarrow \{x_0, x_1\};\ y \leftarrow E(e, x)) \le$$

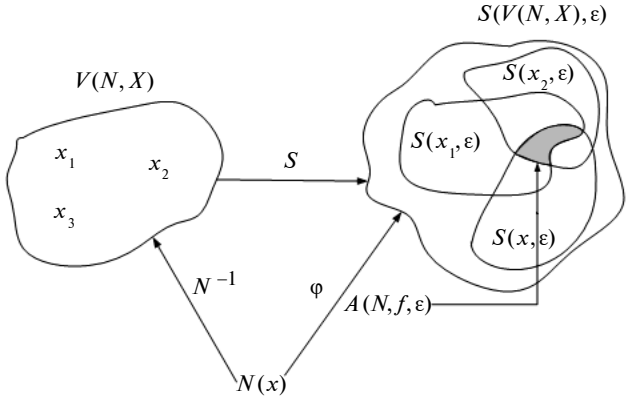
$$\le \frac{1}{2} + \frac{1}{Q(k)}.$$

Модель, заснована на загальній теорії оптимальних алгоритмів (ЗТОА). На основі аналізу існуючих моделей стійкості можна побудувати більш загальну модель, яка до того ж є більш адекватною при дослідженні асиметричних криптосистем, які практично використовуються. Розглянемо її детальніше. Введемо такі позначення. Нехай задано множини X, Y і нехай 2^Y – клас усіх підмножин множини Y. У статті [11] розглядається оператор $S : X \times \Re_+ \to 2^Y$, де $\Re_+ = [0, \infty)$ – так званий оператор розв'язку, який має такі властивості:

$$S(x, 0) \ne \varnothing \quad \forall x \in X,$$

$$\delta_1 \le \delta_2 \Rightarrow S(x,\delta_1) \subset S(x,\delta_2) \quad \forall \delta_1, \delta_2 \in \Re_+, \ x \in X.$$

Для заданого $\varepsilon \ge 0$ елемент $y \in Y$, який задовольняє умову $y \in S(x,\varepsilon)$, 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 y (рисунок).



Інформаційний оператор і оператор розв'язку

Якщо множина $V(N,x) = \{\tilde{x} \in X : N(\tilde{x}) = N(x)$ всіх елементів $\tilde{x}$, які є нерозрізненими, за допомогою $N(x)$ є одноточковою, то оператор N встановлює функціональну залежність між множинами X, Y і називається повним. Оператор розв'язку, 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 $\delta_1 \le \delta_2 \Rightarrow A(N,x,\delta_1) \subset A(N,x,\delta_2)$. Тоді величини $r(N,x) = \inf\{\delta : A(N,x,\delta) \ne \varnothing\}$ і $r(N) = \sup_{x \in X} r(N,x) (= \inf\{\delta : A(N,x,\delta) \ne \varnothing \ \forall x \in X\})$ визначають нижні оцінки точності розв'язків, які можуть бути досягнуті при умові неповного інформаційного оператора. На множині ідеальних алгоритмів $\Phi(N) : N(x) \to G$ із визначеними локальною $e(\varphi,N,x) = \inf\{\delta : \varphi(N(x)) \in A(N,x,\delta)\}$ і глобальною $e(\varphi,N) = \sup_{x \in X} \varepsilon(\varphi,N,x)$ похибками інформація $N(x)$ дає можливість знайти ε-наближення для будь-якого $x \in X$ тоді і тільки тоді, коли виконується одна з умов:

$$r(N) < \varepsilon,$$

$$r(N) = \varepsilon, \exists \varphi : \varphi(N(x)) \in S(x, e(\varphi,N)) \ \forall x \in X.$$

У випадку наближеної інформації N_ρ (ρ – міра похибки) результати для нижніх оцінок визначаються аналогічно:

$$r(N_\rho) < \varepsilon,$$

$$r(N_\rho) = \varepsilon, \exists \varphi : \varphi(N_\rho(x)) \in S(x, e(\varphi,N_\rho)) \ \forall x \in X.$$

На відміну від точного інформаційного оператора оператор N_ρ визначається через оператор інформаційної помилки $E : H \times \Re_+ \to 2^H$, який має такі властивості:

$$E(h,0) \ne \varnothing \ \forall h \in H,$$

$$\delta_1 \le \delta_2 \Rightarrow E(h,\delta_1) \subset S(h,\delta_2) \quad \forall \delta_1, \delta_2 \in \Re_+, \ h \in H.$$

Наближений оператор $N_\rho : X \to H$ задовольняє умову

$$N_\rho(x) \in E(N(x),\rho) \ \forall x \in X.$$

Зауважимо, що якщо точний інформаційний оператор N є неповним, то N_ρ також неповний; якщо ж N є повним, то N_ρ може бути як повним, так і неповним. Якщо оператор N_ρ є повним, то $r(N_\rho) = 0$.

Позначимо X множину відкритих текстів. Тоді $N : X \to Y$ – оператор, який відображає криптографічне перетворення, $S : X \times \Re_+ \to 2^G$ – оператор криптографічного аналізу, G – множина критеріїв належності до множини X. Як $\Phi(N(X))$ вибираємо множину ідеальних алгоритмів φ реалізації оператора криптоаналізу. При цьому умова ідеальної стійкості визначається як $r(N(X)) \ge \varepsilon > 0$, де $r(N(X))$ – радіус інформації $N(X)$. Визначимо введену модель стійкості як "модель ЗТОА".

Справедливі такі теореми.

Теорема 1. Для криптосистем, ідеально стійких у моделі ЗТОА, усі криптографічні перетворення мають властивість не зберігати гомоморфізм.

З теореми 1 випливає така теорема.

Теорема 2. Криптосистема, ідеально стійка в моделі ЗТОА, є також стійкою в розумінні поліноміальної нерозрізненості.

Висновки

Математична модель на базі ЗТОА є більш загальним визначенням стійкості порівняно з моделями стійкості в розумінні поліноміальної нерозрізненості, збереження гомоморфізму та анонімності відкритих ключів, які розглядалися в даній статті. На відміну від моделі анонімності ключів, де просто вибирається множина відкритих ключів, в моделі ЗТОА свідомо "спотворюються" біти відкритого ключа (можливо, і адаптивно), а наявність у порушника навіть вибраної пари "криптограма/відкритий текст" не дає повної інформації про вибраний відкритий ключ, оскільки рандомізація вноситься в зв'язок відкритого та особистого ключів. За загальний вимір стійкості рандомізованих асиметричних криптосистем можна вибрати радіус інформації.

А.М. Кудин

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ СТОЙКОСТИ КРИПТОСИСТЕМ

Исследованы существующие модели криптографических криптосистем с точки зрения определения их стойкости к криптоанализу. Предложена новая математическая модель для оценки стойкости асимметричных криптосистем, которая обобщает существующие подходы.

A.M. Kudin

COMPARATIVE ANALYSES OF MATHEMATICAL MODELS OF SECURITY CRYPTOSYSTEMS

The present study investigates the existing models of security cryptographic systems. Crucially, we propose a novel mathematical model for estimating the security asymmetric cryptosystems. This model generalizes existing approaches to estimation of security asymmetric cryptosystems.

1. *Bellare M., Boldyreva A., Desai A., Pointcheval D.* Key-privacy in public-key encryption // ASIACRYPT. – 2001. – LCNS 2248. – P. 566–582.
2. *Jurgensen H., Robbins L.* Towards foundatioms of cryptography: investigation of perfect secrecy // J. of universal computer science. – 1996. – **2**, N 5. – P. 347–379.
3. *Штарьков Ю.М., Юхансон Т., Смитс Б.Д.М.* О совместной стойкости защиты информации и ключа в секретных системах // Пробл. передачи информации. – 1998. – **34**, вып. 2. – С. 117–127.
4. *Dolev D., Dwork C., Naor M.* Non-malleable cryptography // Proc. of twenty-third annual ACM symposium on theory of computing. – New Orleans, Lousiana, 1991. – P. 542–552.
5. *Goldwasser S., Bellare M.* Lecture Notes on Cryptography. – Cambridge; Massachusetts, 2001. – 283 p.
6. *Abadi M., Rogaway P.* Reconciling two views of cryptography (The computational soundness of formal encryption) // J. of Cryptology. – 2002. – **15**, N 2. – P. 103–127.
7. *Rueppe R., Rainer A.* Analysis and design of stream ciphers. With a foreword by James L. Massey. Communications and Control Engineering Series. – Berlin: Springer-Verlag, 1986. – 244 p.
8. *Зубов А.Ю.* Криптографические методы защиты информации. Совершенные шифры: Учеб. пос. – М.: Гелиос АРВ, 2005. – 192 с.
9. *Yao A.C.* Theory and application of trapdoor functions // 23rd Annual symposium on foundations of computer science. – Chicago, 1982. – P. 80–91.
10. *Успенский В., Верещагин Н., Шень А.* Колмогоровская сложность. – М., 2004. – 326 с.
11. *Кудин А.М.* Об одном классе криптографических преобразований для модели источников информации Колмогорова // Пр. міжнар. симп. "Питання оптимізації обчислень ПОО–XXXV". – К.: Ін-т кібернетики ім. В.М. Глушкова НАН України, 2009. – Том 1. – С. 394–399.

Рекомендована Радою
Фізико-технічного інституту
НТУУ "КПІ"

Надійшла до редакції
18 травня 2010 року