УДК 681.3.06

О. Ю. Іохов **В. Г. Малюк** **І. І. Сидоренко**

ВИЗНАЧЕННЯ ШЛЯХІВ ПІДВИЩЕННЯ ІМІТОСТІЙКОСТІ СИГНАЛІВ ПОПЕРЕДЖЕННЯ СИСТЕМ ОХОРОНИ НГУ НА АТОМНИХ ЕЛЕКТРОСТАНЦІЯХ

Досліджено шляхи підвищення імітостійкості сигналів попередження систем охорони НГУ на об'єктах критичної інфраструктури. Виконано аналіз автентичності повідомлень з конструктивними елементами МАС кодів на основі сімей хеш-функцій. Зроблений висновок, що практичні схеми хешування повинні включати класи хеш-функцій з великим коефіцієнтом стиснення для даних можливо дуже великого об'єму. Наведені оцінки колізійної стійкості для схем універсального хешування за найкращими алгебраїчними кривими з великим числом точок і максимальними кривими.

К л ю ч о в і с л о в а: автентичності повідомлень, алгебраїчні криві, хеш-функції, універсальне хешування.

Постановка проблеми. Сучасні інформаційно-комунікаційні технології все більш широко використовуються для обслуговування об'єктів критичної інфраструктури, таких як атомні електростанції (АЕС). Разом із численними перевагами в експлуатаційній безпеці й ефективності розвиток інформаційних технологій обумовив виникнення нових загроз безпеці критичної інфраструктури, зокрема зростає кількість та потужність кібератак, мотивованих інтересами окремих держав, організацій та груп осіб.

Саме з цих причин відповідно до Стратегії кібербезпеки України [1] необхідно забезпечити захист інформації на об'єктах критичної інфраструктури. Важливим кроком на шляху створення сучасної системи кіберзахисту України стало прийняття Постанови Кабінету Міністрів України від 19 червня 2019 року № 518 "Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури" [2], якою визначені загальні вимоги до кіберзахисту об'єктів критичної інфраструктури; встановлені обов'язкові заходи забезпечення захисту від кібератак та запобігання порушенню конфіденційності, цілісності та доступності інформаційних ресурсів.

Оскільки АЕС є важливими державними об'єктами, фізичний захист яких забезпечують військові частини Національної гвардії України (НГУ) [3], актуальною стає задача забезпечення конфіденційності та цілісності повідомлень, якими обмінюються частини і підрозділи НГУ через систему оповіщення потенційно небезпечних об'єктів [4]. Для вирішення цієї задачі використовується імітостійке кодування даних, яке дає можливість перевірити, чи були змінені дані третьою стороною. Ймовірність того, що дані були змінені, слугує мірою імітостійкості шифру.

Забезпечити імітостійкість систем передавання даних можливо на основі рішення взаємопов'язаної сукупності задач захисту інформації. Якість їх рішення значною мірою визначається криптографічними алгоритмами шифрування, цифрового підпису, хешування і формування кодів автентифікації, що використовуються.

Коди автентифікації повідомлень (МАС коди), відомі також як коди автентичності повідомлень, є криптографічними примітивами, що використовуються для забезпечення цілісності та автентичності даних. Можна виділити три основні підходи до побудови кодів автентифікації повідомлення [5]:

1) із застосуванням блокових шифрів;

2) на основі безключових хеш-функцій;

3) з використанням сім'ї універсальних хеш-функцій.

Для універсального хешування з великим коефіцієнтом стиснення перспективними є схеми з алгеброгеометричними кодами.

Вперше алгеброгеометричний підхід до побудови кодів був запропонований В. Д. Гоппою у 1981 році [6]. У працях [7–10] показано, що за алгеброгеометричними кривими можна будувати коди з дуже добрими асимптотичними властивостями. Доведено існування нескінченних серій q лінійних кодів, параметри яких (при q та $N \to \infty$) лежать вище межи Варшамова–Гільберта. Одними з кращих у цьому класі є коди з використанням кривих Ерміта.

Мета статті – дослідження методів побудови MAC кодів імітозахисту на основі алгеброгеометричних кривих, які забезпечують підвищення імітостійкості передавання даних.

Виклад основного матеріалу. За Принелем [11], MAC код – це функція відображення $h: K \times M \to R$, де $K = \{0,1\}^k$ – простір ключів; $M = \{0,1\}^*$ – простір повідомлень та $R = \{0,1\}^n$ – простір MAC значень для $k, n \geq 1$. Для заданих значень ключа $k \in K$ та повідомлення $X \in M$ функція виробляє MAC значення $Y \in R$.

Більшість MAC кодів – ітеративні конструкції. Проведемо дослідження методів побудови ітераційних MAC кодів.

Узагальнена модель ітеративного MAC коду для t підблоків використовує функцію стиснення f, попереднє розбиття даних X на підблоки X_i і зв'язок за зворотним входом проміжних результатів обчислень хеш-значень та визначається таким алгоритмом ітеративних обчислень:

$$\begin{gathered} H_0 = IV_k, \\ H_i = f_{k(H_{i-1}, X_i), 1 \leq i \leq t}, \\ h(k.X) = g(H_t). \end{gathered} \tag{1}$$

Секретний ключ k може використовуватися у векторі ініціалізації IV, у функції стиснення f та у вихідному перетворенні g.

Конструктивними елементами MAC кодів на основі сімей хеш-функцій є хеш-функції, функції стиснення та ітераційні хеш-функції. Основні визначення і властивості хеш-функції наведемо в поданні Рогавея [12].

Визначення 1 [12]. Хеш-функцією називається функція відображення $h: D \to R$, де область значень $D = \{0,1\}^*$, а $R = \{0,1\}^n$ для деякого $n \geq 1$.

Визначення 2 [12]. Функцією стиснення називається функція відображення $f: D \to R$, де $D = \{0,1\}^a \times \{0,1\}^b$ та $R = \{0,1\}^n$ для деяких $a, b, n \geq 1$ та $a + b \geq 1$.

Визначення 3 [12]. Ітераційною хеш-функцією від функції стиснення $f: \left(\{0,1\}^a \times \{0,1\}^b\right) \to \{0,1\}^n$ є хеш-функція $h: \left(\{0,1\}^b\right)^* \to \{0,1\}^n$, визначена $h(X_1 ... X_t) = H_t$, де $H_i = f(H_{i-1}, X_i)$ при $1 \leq i \leq t (H_0 = IV)$.

Практичні схеми хешування повинні включати класи хеш-функцій з великим коефіцієнтом стиснення для даних, об'єм яких повинен мінятися в достатньо широкому діапазоні [15; 16].

З цією метою цікавими є такі сім'ї хешей:

– універсальні класи хеш-функцій;

– схеми універсального хешування на основі довгих алгеброгеометричних кодів;

– композиційні схеми універсального хешування.

Для вирішення задачі ефективного використання MAC кодів необхідно дослідити властивості існуючих схем універсального хешування.

Ідея універсального хешування була запропонована Картером і Вегманом у 1981 році для побудови колізійно стійких і високошвидкісних кодів автентифікації.

Універсальні сім'ї хеш-функцій є об'єктами польових структур, характеризуються прозорими комбінаторними властивостями і мають доказову секретність. Наведемо визначення універсальних класів і розглянемо властивості комбінаторних схем. Основні положення узяті з праць Рогавея [12], Картера і Вегмана [13] та Стінсона [14].

Визначення 4 [12, 14]. $(N;n,m)$ хеш-сім'я є множина з N функцій H такі, що

$$h: A \to B, \tag{2}$$

де $h \in H$, $|A| = n$ та $|B| = m$, $n \geq m$.

Визначення 5 [12, 14]. $(N;n,m)$ хеш-сім'я є ε універсальною, якщо для будь-яких двох різних елементів $x_1, x_2 \in A$ існує найбільша кількість εN функцій $h \in H$ таких, що $h(x_1) = h(x_2)$. Абревіатура $\varepsilon - U$ використовується для позначення ε універсальних хеш-функцій.

Вочевидь, якщо h вибирається випадково із заданого $\varepsilon - U(N;n,m)$ хеш-сім'ї, тоді ймовірність колізії хеш-значень для двох різних вхідних повідомлень $x_1, x_2 \in A$ не перевищує ε.

$$\Pr_{h \in H}\left[h(x_1) = h(x_2)\right] \leq \varepsilon. \tag{3}$$

Насамперед, визначення універсальних хеш-функцій Картера і Вегмана було запропоновано для $\varepsilon = 1/m$. Наступні визначення – це узагальнення попереднього.

Визначення 6 [13]. H є ε майже універсальною сім'єю хеш-функцій ($\varepsilon - AU(N;n,m)$), якщо $\Pr_{h \in H}\left[h(x_1) = h(x_2)\right] \leq \varepsilon$ для $x_1, x_2 \in A$, $x_1 \neq x_2$, $1/m \leq \varepsilon \leq 1$.

Наступні визначення стосуються класів хеш-функцій суворої універсальності.

Визначення 7 [13]. H є ε суворо універсальною сім'єю хеш-функцій ($\varepsilon - SU(N;n,m)$), якщо для всіх $x_1, x_2 \in A$, $x_1 \neq x_2$ та всіх $a, b \in B$, $\Pr_{h \in H}\left[h(x_1) = a, h(x_2) = b\right] = \varepsilon$, $\varepsilon = 1/B^2$.

Визначення 8 [13]. H є ε майже суворо універсальною сім'єю хеш-функцій ($\varepsilon - ASU(N;n,m)$), якщо для всіх $x_1, x_2 \in A$, $x_1 \neq x_2$ і всіх $a, b \in B$, $\Pr_{h \in H}\left[h(x_1) = a, h(x_2) = b\right] \leq \varepsilon$.

Однією з найбільш відомих універсальних сімей хеш-функцій є PolyCW хешування (polynomial Carter–Wegman hashing) [13]. Головна властивість PolyCW функції визначається фундаментальною теоремою алгебри: многочлен, відмінний від нуля, степеня не менше k, має не менше k коренів. Імовірність колізії для поліноміальної хеш-функції обмежується відношенням k/q, де q – просте число, визначальне поле Z_q для обчислення многочленів. Множина ключів визначається значенням q. Чим більше розмір ключового простору, тим більшу кількість слів можна хешувати до досягнення допустимої імовірності колізії. При збільшенні q зростають тимчасові затрати на обчислення хеш-значень у Z_q. При русі q від 2^{32} до 2^{64} тимчасові витрати збільшуються у два рази. Обмеження, пов'язані із обчисленнями у великих полях Z_q, частково знімаються в конструкції сповзаючого поліноміального хешування RPHash (ramped polynomial hashing), використаного в UMAC алгоритмі [15; 16].

Ще одним підходом, що зменшує суперечність між обчислювальними витратами у великих полях і необхідністю забезпечити на великій довжині повідомлення мале значення ймовірності колізії, є застосування універсального хешування з алгеброгеометричними кодами (АГК) [17–20]. У схемах з АГК (n,k,d) імовірність колізії визначається значенням $1 - d/n$. Для відомих до нинішнього часу АГК імовірність колізії обмежується в кращому випадку значенням, що оберненопропорційно квадрату розмірності поля Z_q. Тому цікавою є поведінка параметрів хеш-функції на основі алгеброгеометричних кодів, особливо за різних умов їх використання.

Застосування алгеброгеометричних кодів для побудови універсальних сімей хеш-функцій забезпечує найкращі співвідношення між розміром хеш-значень та ймовірністю колізії при обчисленнях у кінцевих полях. Зв'язок між універсальною сім'єю хеш-функцій і кодовими схемами вперше був визначений Бієрбрауером, Джохансоном, Кабатіанські та Смітом [17].

Теорема [17]. Якщо існує $(N,K,D)_q$ код, тоді існує $\left(1-\frac{D}{N}\right)-AU(N;K,q)$ хеш-сім'я. І навпаки, якщо е $\varepsilon-U(N;n,m)$ хеш-сім'я, тоді існує $(N;n,N(1-\varepsilon))$ код.

Аналіз загальних характеристик АГК показав, що найкращі властивості з погляду на їх кодову відстань та складність обчислення мають розширений код Ріда–Соломона, коди з використанням кривих Ерміта та коди з використанням кривих Судзукі [18–20].

Універсальне хешування за РС кодами (Rsh) в алгеброгеометричній інтерпретації має таке подання. Нехай F – алгебраїчне покриття F_q. Точки ξ визначаються гомогенними координатами (x,y), мають значення $P_i=(\alpha_i,1)$, $0\le i\le q-1$ та $Q=(1,0)$ – особлива точка (точка невизначеності). Нехай $f\in F_q(\xi)$ – раціональні функції, визначені в кожній P_i з коефіцієнтами у F_q і мають полюс порядку менше, ніж m у точці Q, і немає інших полюсів. Раціональна функція f має вигляд $\frac{\alpha(x,y)}{\beta(x,y)}$, де $\alpha(x,y)$ та $\beta(x,y)$ – гомогенні поліноми степеня $<k$. Алгеброгеометричний код визначимо як

$$C=\left\{\left(f(P_0),f(P_1),...,f\left(P_{q-1}\right)\right)\middle|f\in L(mQ)\right\}. \tag{4}$$

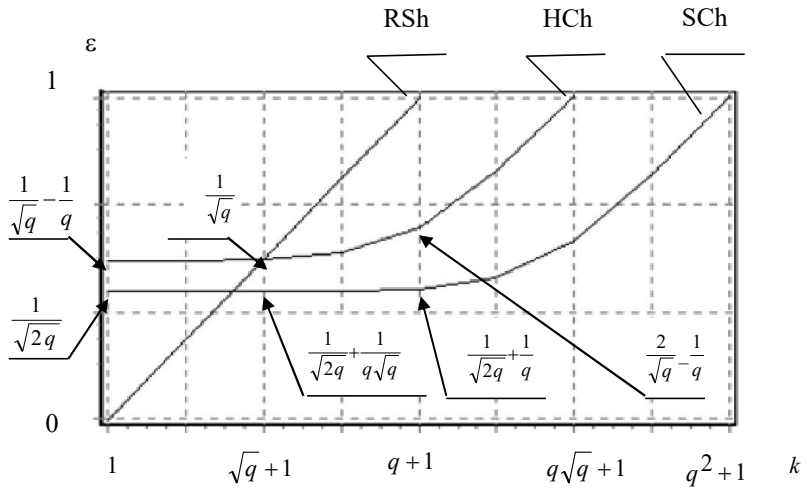
Код $\tilde{N}$ має розмірність простору $L(mQ)$, $g=0$, $k=\dim C=m-g+1=m+1$ і мінімальну відстань $d\ge n-m$. Таким чином, отримаємо РС код $(q,k,q-k+1)$ у алгеброгеометричній інтерпретації і універсальний клас хеш-функцій $\frac{k-1}{q}-U\left(q,q^k,q\right)$.

Алгеброгеометричне хешування за кодами Ерміта (Hch) використовує криву Ерміта, що визначається рівнянням $y^{\sqrt{q}}+y=x^{\sqrt{q}+1}$ над квадратичним полем $F_{q=p^2}$. Число точок кривої $N=q\sqrt{q+1}$, сім'я $g=\sqrt{q}\left(\sqrt{q}-1\right)$. Нехай $P_\infty=(0:1:0)$ і $G=mP_\infty$. Базис простору $L(mQ)$ задається функціями $\left\{x^i\cdot y^j:i\sqrt{q}+j\left(\sqrt{q}+1\right)\le m\right\}$. Для алгеброгеометричного кодування код Ерміта має параметри $\left[\sqrt{q},k,d\ge q\sqrt{q}-k+1-g\right]$, що обумовлюють параметри універсального хешування $\frac{1}{\sqrt{q}}\left(\frac{k-1}{q}+1-\frac{1}{\sqrt{q}}\right)-U\left(q\sqrt{q},q^k,q\right)$.

Крива Судзукі $y^q-y=x^{q_0}\left(x^q-x\right)$ визначена над полем F_q, $q=2q_0^2$, $q_0=2^s$ сім'ї $g=q_0(q-1)$ і має число точок $N=q^2+1$. Базис простору $L(\rho_\ell P_0)$ задається функціями

$$\left\{w^j\cdot v^j\cdot y^t\cdot x^r:i(q+2q_0)+j(q+2q_0+1)+t(q+q_0)+r\cdot q\le\rho_\ell\right\}. \tag{5}$$

Залежність ймовірності колізій для АГК конструкцій від довжини хешуємого повідомлення зображена на рисунку.



Залежність ймовірності колізії для універсального хешування з АГК
від довжини повідомлення

Аналіз залежності асимптотичних границь ймовірності колізії $\varepsilon(\mathrm{k})$ для конструкцій з АГК показує, що при $\mathrm{k} < \sqrt{\mathrm{q}}$ перевагу мають RS коди. При $\mathrm{k} > \sqrt{\mathrm{q}}$ слід віддати перевагу HC і SC кодам. Універсальне хешування з кодами Судзукі має меншу ймовірність колізії порівняно з кодами Ерміта на всіх довжинах повідомлень. Разом з тим відсутність практичного, ефективного алгоритму обчислення хеш-значень для схеми з кодами SC обмежує їх застосування в схемах універсального хешування.

Схеми з HC кодами для $\mathrm{k} = \mathrm{q} + 1$ мають значення $\varepsilon(\mathrm{q}+1) = \frac{2}{\sqrt{\mathrm{q}}} - \frac{1}{\mathrm{q}}$, при подальшому зростанні $\mathrm{k} \to \mathrm{q}\sqrt{\mathrm{q}}$ ε майже лінійно прямує до 1. Таким чином, застосування АГК для хешування даних дозволяє забезпечити хешування повідомлень завдовжки $\mathrm{k} \le \sqrt{\mathrm{q}}$ з імовірністю колізії, яка не перевищує значення $\varepsilon = \frac{2}{\sqrt{\mathrm{q}}}$, і складністю обчислень, що визначається арифметикою поля $\mathrm{F_q}$ і алгоритмом побудови кодових слів.

Складність обчислення хеш-функції $\mathrm{RSh_q}$ для повідомлень завдовжки k слів складе k операцій додавання і множення. Застосування $\mathrm{HCh_q}$ хешування потребує (це не складно показати) приблизно $\mathrm{k} + \sqrt{\mathrm{q}}$ операцій додавання і множення [18–20]. Таким чином, $\mathrm{RSh_q}$ хешування ефективніше щодо витрат на обчислення, але для довжин даних, які перевищують значення $\mathrm{k} > \sqrt{\mathrm{q}}$, програє за ймовірністю колізії $\mathrm{HCh_q}$ схемі. Порівняльний аналіз параметрів схем хешування з розглянутими кодовими конструкціями наведений у таблиці.

Параметри розглянутих схем хешування

Схема хешування	Асимптотичні оцінки ймовірності колізії ε	Поле обчислень	Довжина хешуємих даних
$\mathrm{RSh_q}$	$\frac{\mathrm{k}-1}{\mathrm{q}}$	$\mathrm{F_q}$, $\mathrm{q} = \mathrm{p}^{\mathrm{m}}$	$1 \le \mathrm{k} \le \mathrm{q}$
$\mathrm{HCh_q}$	$\frac{1}{\sqrt{\mathrm{q}}}\left(\frac{\mathrm{k}-1}{\mathrm{q}}+1-\frac{1}{\sqrt{\mathrm{q}}}\right)$	$\mathrm{F_q}$, $\mathrm{q} = \mathrm{p}^2$	$1 \le \mathrm{k} \le \mathrm{q}\sqrt{\mathrm{q}}$
$\mathrm{SCh_q}$	$\frac{1}{\mathrm{q}}\left[\frac{\mathrm{k}-1}{\mathrm{q}}+\sqrt{\frac{\mathrm{q}}{2}}\right]$	$\mathrm{F_q}$, $\mathrm{q} = \mathrm{p}^{2\mathrm{f}+1}$	$1 \le \mathrm{k} \le \mathrm{q}^2$

Недолік хешування з АГК полягає в тому, що ймовірність колізії зростає майже лінійно із зростанням довжини повідомлення, а її зменшення можливе шляхом обмеження довжини повідомлення, що хешується, або збільшення розміру поля обчислення хеш-значення Z_q.

Отже, для побудови хеш-схем найбільш цікавими є АГК дуже великої довжини, ефективні в обчислювальному відношенні. До таких практичних кодів віднесені коди з використанням кривих Ерміта.

Висновки

Проведене дослідження методів побудови МАС кодів імітозахисту на основі алгеброгеометричних кодів показало, що одним із шляхів підвищення імітостійкості передавання даних є застосування кодів з використанням кривих Ерміта.

Практичні схеми хешування повинні включати класи хеш-функцій з великим коефіцієнтом стиснення для даних можливо дуже великого об'єму. Для цих цілей цікавими є сім'ї хешей на основі довгих алгеброгеометричних кодів. У схемах з АГК кодами (n,k,d) імовірність колізії визначається значенням $1-d/n$. Лінійне зростання ймовірності колізії для RShp хешування обмежує розмір хешуємого повідомлення.

Викладена теорія універсального хешування з алгеброгеометричними кодами Ріда–Соломона і кодами з використанням кривих Ерміта здатна забезпечити необхідні показники ймовірності колізії хеш-функцій.

Перелік джерел посилання

1. Про Стратегію кібербезпеки України: Указ Президента України від 15.03.2016 р. № 96/2016. URL: *https:// zakon.rada.gov.ua/laws/show/96/2016* (дата звернення: 08.11.2019).

2. Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019 р. № 518. *Офіційний вісник України*. 2019. № 50. С. 53.

3. Орлов М. М. Оперативне застосування військ Національної гвардії України у системі фізичного захисту атомних електростанцій. *Забезпечення службово-бойової діяльності Національної гвардії України*: зб. тез VI наук.-практ. конф. м. Харків, 9 квіт. 2015 р. Харків: НАНГУ, 2015. С. 41–42.

4. Білоусов С. І. Об'єктові, локальні та спеціальні автоматизовані системи оповіщення цивільного захисту: навч. посіб. Одеса: ОНАЗ ім. О. С. Попова, 2013. 44 с.

5. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія: монографія. Харків: ХНУРЕ: Форт, 2012. 878 с.

6. Гоппа В. Д. Коды на алгебраических кривых. *Доклады АН СССР*. 1981. Т. 259. № 6. С. 1289–1290.

7. Влэдуц С. Г., Манин Ю. И. Линейные коды и модулярные кривые. *Современные проблемы математики*. Москва: ВИНИТИ, 1984. Т. 25. С. 209–257.

8. Влэдуц С. Г., Ногин Д. Ю., Цфасман М. А. Алгеброгеометрические коды. Основные понятия. Москва: МЦНМО, 2003. 504 с.

9. Ruud Pellikaan. Asymptotically good sequences of curves and codes. *Proc. 34th Allerton Conf. on Communication, Control and Computing*, Urbana-Champaign, October 2–4, 1996. P. 276–285.

10. Voss, Tom Hoholdt. An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zink bound. The first steps. *IEEE Trans. Info. Theory*. 1997. vol. IT-43. P. 128–135.

11. Preneel B., Rijmen V. "Cryptographic primitives for information authentication state of the art" in State of the Art in Applied Cryptography. *Lecture Notes in Computer Science*. Springer-Verlag. 1998. № 1528. P. 50–105.

12. Black J., Rogaway P. Ciphers with arbitrary finite domains. Proceedings of CT-RSA'02. *Lecture Notes in Computer Science SpringerVerlag*. 2002. № 2271. P. 114–130. URL: www.cs.ucdavis.edu/~rogaway/ papers/subset.htm.

13. Carter J. L., Wegman M. N. Universal classes of hash functions. *J. Computer and System*. 1979. Sci. 18. P. 143–154.

14. Stinson D. Universal hashing and authentication codes. *Design, Codes and Cryptography*. 1994. Vol. 4. P. 369–380.

15. UMAC: Fast and secure message authentication / J. Black et al. *In Advances in Cryptology "CRYPTO" 99*: Lecture Notes in Computer Science, Springer-Verlag. 1999. Vol. 1666. P. 216–233.

16. UMAC / T. Krovetz et al. *Primitive submitted to NESSIE*. 2000. Sept. P. 157–160.

17. On families of hash functions via geometric codes and concatenation / J. Bierbrauer et al. *Advances in Cryptology, CRYPTO '93 Proceedings*. Springer-Verlag. 1994. P. 331–342.

18. Халимов Г. З., Кузнецов А. А. Аутентификация с применением алгеброгеометрических кодов. *Радиотехника*. 2001. Вып. 119. С. 103–109.

19. Халимов Г. З., Иохов А. Ю. Аутентификация с применением эрмитовых кодов. *Вестник ХПИ*. Харьков, 2005. Вып. 9. С. 26–32.

20. Халимов Г. З., Иохов А. Ю. Универсальное хеширование по рациональным функциям кривой Эрмита. *Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку*: зб. тез доп. міжнародної наук.-практ. конф., м. Харків, 17–18 берез. 2011 р. Харків: Акад. ВВ МВСУ, 2011. С. 48–51.

Стаття надійшла до редакції 20.11.2019 р.

УДК 681.3.06

А. Ю. Иохов, В. Г. Малюк, И. И. Сидоренко

ОПРЕДЕЛЕНИЕ ПУТЕЙ ПОВЫШЕНИЯ ИМИТОСТОЙКОСТИ СИГНАЛОВ ПРЕДУПРЕЖДЕНИЯ СИСТЕМ ОХРАНЫ НГУ НА АТОМНЫХ ЭЛЕКТРОСТАНЦИЯХ

Исследованы пути повышения имитостойкости сигналов предупреждения систем охраны НГУ на объектах критической инфраструктуры. Выполнен анализ подлинности сообщений с конструктивными элементами MAC кодов на основе семейств хеш-функций. Сделан вывод, что практические схемы хеширования должны включать классы хеш-функций с большим коэффициентом сжатия для данных возможно очень большого объема. Представлены оценки коллизионной устойчивости для схем универсального хеширования по лучшим алгебраическим кривым с большим числом точек и максимальным кривым.

К л ю ч е в ы е с л о в а: подлинность сообщений, алгебраические кривые, хеш-функции, универсальное хеширование.

UDC 681.3.06

O. Iohov, V. Maliuk, I. Sydorenko

DETERMINATION OF WAYS OF SPOOFING RESISTANCE IMPROVEMENT OF WARNING SYSTEMS OF NGU SECURITY SYSTEMS AT NUCLEAR POWER LANTS

An important part of the combat activity of units of the National Guard of Ukraine is the physical protection of important state critical infrastructure facilities. The development of modern information technologies leads to the emergence of new threats to the security of such facilities, in particular, the number and power of cyber-attacks motivated by the interests of individual states, organizations and groups of people is growing. This determines the relevance of ensuring the confidentiality and integrity of messages exchanged between units of the National Guard of Ukraine through a warning system with potentially dangerous objects. To solve this problem, imitation-resistant data encoding is used, which makes it possible to check whether the data has been changed by a third party. The likelihood that the data has been changed serves as a measure of the resistance of the cipher.

Ensuring the simulated resistance of data transmission systems is possible on the basis of solving an interconnected set of information protection tasks. The quality of solving security problems is largely

determined by cryptographic algorithms for encryption, digital signature, hashing and generation of authentication codes used.

A study of ways to increase the spoofing resistance of warning signals of the guard systems of the National Guard of Ukraine at critical infrastructure facilities was conducted.

An analysis of the authenticity of messages with constructive elements of MAC codes based on hash function families is made. It is concluded that practical hashing schemes should include hash classes with a large compression ratio for data of very large volumes as possible. For these purposes, hash families on the basis of long algebraic geometric codes are of interest.

An analysis of the general characteristics of algebraic-geometric codes showed that the best properties in terms of their code distance and computational complexity are the extended Reed-Solomon code, codes on Hermite curves, and codes on Suzuki curves. Collision stability estimates are presented for universal hashing schemes for the best algebraic curves with a large number of points and a maximum curve.

The presented theory of universal hashing with Reed-Solomon algebraic-geometrical codes and codes on Hermite curves shows the ability to provide the necessary measure of the probability of collision of hash functions. Since a linear increase in collision probability for Reed-Solomon hashing limits the size of the hashed message, one of the ways to increase the simplicity of data transmission is to use codes on Hermite curves.

K e y w o r d s: message authenticity, algebraic curves, hash functions, universal hashing

Іохов Олександр Юрійович – кандидат технічних наук, старший науковий співробітник, завідувач кафедри військового зв'язку та інформатизації Національної академії Національної гвардії України.

https://orcid.org /0000-0002-1718-0138

Малюк Віктор Григорович – кандидат технічних наук, професор кафедри військового зв'язку та інформатизації Національної академії Національної гвардії України.

https://orcid.org/0000–0001–6510–3025

Сидоренко Ірина Ігорівна – кандидат педагогічних наук, доцент кафедри фундаментальних дисциплін Національної академії Національної гвардії України.

https://orcid.org/0000-0001-7434-682X