Секція 1.SEC
(Безпека комп'ютерних систем та мереж. Відмовостійкі розподілені обчислення..)

Section 1. SEC
(Securityofcomputersystemsandnetworks. Fault-tolerantdistributedcomputing.)

Марковський Олександр Петрович,
Сербін Олександр Дмитрович

АЛГОРИТМ ЦИФРОВОГО ПІДПИСУ З ВИКОРИСТАННЯМ ПОЛІНОМІАЛЬНОЇ АРИФМЕТИКИ НА ПОЛЯХ ГАЛУА

ADIGITAL SIGNATURE ALGORITHM BASEDON POLINOMIAL ARIFMETIC SOFGALO ISFIELDS

Based on the cyclic properties of the exponential operation on the Galois fields, a new method for forming a digital signature is proposed. The constructivity of the proposed method is proved. It is theoretically and experimentally proved that the proposed method allows to accelerate the formation and verification of a digital signature in comparison with known methods.

Key words: digital signature, Galois fields, data protection, irreversible transformations.

На основі циклічних властивостей операції експоненціювання на полях Галуа запропоновано новий метод формування цифрового підпису. Доведена конструктивність запропонованого методу. Теоретично та експериментально доведено, що запропонований метод дозволяє прискорити формування та перевірку цифрового підпису у порівнянні з відомими методами.

Ключові слова: цифровий підпис, поля Галуа, захист даних, незворотні перетворення.

Актуальність теми дослідження. Екстенсивний розвиток і зростаюча доступність Інтернету в останні десятиліття призводять до значного поглиблення взаємодії між віддаленими користувачами. У багатьох сферах людської діяльності, зокрема в банківській сфері, відбувається перехід від паперової форми документів до цифрової, що значно підвищує оперативність їх обробки. Необхідною умовою якісної взаємодії сторін за участю цифрових документів є застосування ефективних механізмів контролю їх цілісності та авторства. Ключову роль серед цих механізмів займають схеми формування та перевірки цифрового підпису. З плином часу та розвитком інформаційних технологій змінюються також способи взаємодії віддалених користувачів, що розширює область застосування цифрового підпису, наприклад для контролю автентичності повідомлень у сервісах для обміну повідомленнями, та, посилює потребу

в ефективних механізмах захисту. З появою і розвитком хмарних технологій широкому колу користувачів стають доступними значні за обсягом обчислювальні ресурси, що можуть бути використані зловмисниками для зламу існуючих алгоритмів цифрового підпису. Потенціал хмарних технологій опосередковано впливає на зниження криптографічної стійкості існуючих алгоритмів та порушує баланс сил у світі інформаційної безпеки; це вимагає пошуку адекватних рішень щодо вдосконалення існуючих криптографічних методів, в тому числі і технології цифрового підпису.

Таким чином, проблема підвищення ефективності і захищеності алгоритмів формування цифрового підпису є актуальною з позиції сучасного етапу розвитку комп'ютерних технологій.

Постановка проблеми. Як і для будь-якого механізму криптографічного захисту даних, для оцінки ефективності схеми формування цифрового підпису використовуються два основних критерії[4]:

1. Рівень захищеності або об'єм затрат, необхідний для зламу засобів захисту.

2. Об'єм витрат, необхідних для реалізації цільового рівня захисту.

Будь-який механізм захисту інформації – це компроміс між цими двома критеріями. Формування цифрового підпису – це допоміжна операція, тому її обчислювальна складність має бути невеликою.

В сценарії формування цифрового підпису задіяні наступні сторони. Відправник – сторона, яка створює, підписує та відправляє документ електронний документ по каналу передачі даних отримувачу. Отримувач - сторона, що отримує електронний документ і перевіряє його на автентичність та цілісність шляхом верифікації підпису. Зловмисник – третя сторона, що має доступ до каналу передачі даних і має на меті підробку або спотворення електронного документу[4].

В більшості випадків підписується не сам документ, а його хеш-сигнатура, завдяки чому зменшується об'єм обчислень і вирішуються проблеми сумісності та цілісності[4].

Переважна більшість існуючих схем цифрового підпису є асиметричними, що базуються на обчислювально складних задачах. Перед схемами цифрового підпису ставляться дві головні вимоги:

1. Верифікація підпису повинна проводитися відкритим ключем, відповідним саме тому закритому ключу, який використовувався під час підписання.

2. Створення легітимного цифрового підпису без наявності закритого ключа має бути задачею, складність якої виходить за рамки технічних можливостей сучасних комп'ютерів.

Основу асиметричних схем складають задачі дискретного логарифмування або факторизації чисел. Схема формування цифрового підпису передбачає три етапи:

1. *Генерація ключової пари*. За допомогою алгоритму генерації ключа з набору можливих значень закритих ключів обчислюється закритий ключ та відповідний йому відкритий ключ.

2. *Формування підпису*. Для заданого електронного документа чи повідомлення за допомогою закритого ключа обчислюється підпис.

3. *Верифікація підпису*. Для даних документа та підпису за допомогою відкритого ключа визначається дійсність підпису.

Аналіз останніх досліджень і публікацій. З моменту виникнення першої публікації про алгоритм цифрового підпису було розроблено багато варіантів. Найбільш поширеними на даний момент є алгоритми на основі RSA, Ель-Гамаля та DSA. Вони є також найбільш дослідженими та вважаються достатньо криптостійкими. Ці алгоритми активно використовуються і прийняті за державні стандарти в багатьох країнах світу.

Алгоритм формування цифрового підписуна основі RSA полягає в наступному. Вибираються два великі прості числа p і g Обчислюється їх добуток $n = p \cdot g$. Далі обчислюється функція Ейлера $\varphi(n) = (p - 1) \cdot (g - 1)$. Вибирається ціле число q таке, що $1 < q < \varphi(n)$ та q взаємно просте з $\varphi(n)$. Далі за допомогою Евклідового алгоритму знаходиться число d таке, що $e \cdot d \bmod \varphi(n) = 1 \bmod \varphi(n)$, тобто $d = e^{-1}$. Числа e, nстановлять відкритий ключ, а число d – закритий. Щоб підписати документ або повідомлення m користувач має обчислити хеш-сигнатуру повідомлення $H(m)$ і значення $s = H(m)^d \bmod n$. Перевірка підпису передбачає обчислення $a = s^e \bmod n$. Якщо $a = H(m)$, підпис вважається дійсним[5].

Алгоритм Ель-Гамаля базується на обчислювальній складності операції дискретного логарифмування на скінчених полях. Підпис передбачає наступну послідовність дій. Обчислюється хеш-функція повідомлення mяк$H(m)$. Далі відбувається генерація ключів: генерується випадкове просте число p, підбирається таке g, що є первісним корнем p, вибирається випадкове ціле число x, таке, що $1 < x < p - 1$. Наступним кроком є обчислення $y = g^x \bmod p$. Далі вибирається випадкове числоk таке, що $1 < k <$ (p -1) і обчислюється $r = g^k \bmod p$. Обчислюється число $s = k^{-1} (H(m) - x \cdot r) \bmod (p - 1)$. Пара (r, s) становить підпис повідомлення.

В свою чергу, щоб перевірити підпис треба спочатку перевірити виконання умов $0 < r < p$ і $0 < s < p - 1$. Далі треба обчислити хеш-функцію повідомлення$H(m)$ і перевірити, чи $y^r \cdot r^s = g^{H(m)} \bmod p$. Якщо умова виконується, то підпис вірний[6].

Алгоритм DSA є варіантом алгоритму Ель-Гамаля. В ньому також використовується складність обчислення логарифма в кінцевих полях. Порядок підписування документа виглядає наступним чином. Спочатку вибираються хеш-функція $H(m)$ та число q, що мають однакову бітову розрядність. Далі вибирається просте число p, таке, що $(p - 1)$ ділиться на q. Вибирається таке число g, що його мультиплікативний порядок по модулю p дорівнює q.

Процедура підписування передбачає таку послідовність дій. Вибирається випадкове число k{\displaystyle k\in (0,q)} таке, що $0 < k < q$, вибирається випадкове ціле число x, таке, що $1 < x < p - 1$.Обчислюється {\displaystyle r=(g^{k}\mod p)\mod q}$(r = g^k \bmod p) \bmod q$. Якщо {\displaystyle r=0}$r = 0$, вибирається інше k. Обчислюється {\displaystyles=k^{-1}(H(m)+x\cdotr)\modq}$s = k^{-1}(H(m) + xr) \bmod q$. Якщо {\displaystyle r=0}$s = 0$, вибирається інше k. Підпис становить пара (r, s) загальної довжинизззз{\displaystyle 2N} загальної довжини 2N.

Перевірка підпису відбувається наступним чином. Обчислюється $w = s^{-1} \bmod q$. Обчислюється $u_1 = H(m) \cdot w \bmod q$. Обчислюється $u_2 = r \cdot w \bmod q$. Обчислюється $v = (g^{u1} \cdot y^{u2} \bmod p) \bmod q$. Підпис вірний, якщо $v = r$.

Виділення недосліджених частин загальної проблеми. З плином часу і прогресом комп’ютерних технологій зростає необхідність в підвищенні рівня

захищеності алгоритмів. Рівень захищеності для цього класу алгоритмів може бути підвищений лише за рахунок збільшення розрядності операндів. Разом з тим, добре відомо[5], що збільшення розрядності в двоє призводить до 8-микратного росту обчислювальної складності. Значне підвищення часу реалізації порушує часові нормативи роботи протоколів мережевого захисту.

Головним недоліком алгоритму RSA є обчислювальна складність операції експоненціювання. Також, алгоритм вразливий до різного роду атак при неграмотно підібраних параметрах та при повторному використанні секретних ключів[3].

Використання алгоритму Ель-Гамаля також пов'язане з певними труднощами. Число k необхідно змінювати кожного разу як підписується документ, інакше знаходження закритого ключа стає легкою задачею [6]. Основні обчислювальні затрати йдуть на обчислення експоненти $r = g^k mod p$ та знаходження k^{-1} за алгоритмом Евкліда. Якщо порівнювати алгоритм Ель-Гамаля з RSA, то при тому ж рівні стійкості він оперує з цілими числами на 25% коротше, ніж RSA, але довжина підпису виходить в 1,5 рази більше, що збільшує час її обчислення і посилює вимоги до надійності каналу передачі даних.

У DSA піднесення до степені по модулю та знаходження обернених значень k^{-1} та s^{-1} є, як і у алгоритмі Ель-Гамаля, найбільш ресурсомісткими операціями. Криптостійкість алгоритма сильно так само залежить від якості підбору випадкового параметру k. Повторення параметру k для двох повідомлень робить можливим обчислення ключа третьою стороною [4].

Таким чином, основний недолік існуючих алгоритмів цифрового підпису полягає в тому, що в сучасних умовах їх обчислювальна складність стає на заваді дотримання часових рамок протоколів мережевого захисту інформації малопотужними термінальними пристроями систем комп'ютерного моніторингу та управління.

Постановка завдання. Метою статті є підвищення швидкості формування цифрового підпису за рахунок використання альтернативного математичного базису - скінчених полів Галуа.

Викладення основного матеріалу. Для досягнення поставленої мети – підвищення швидкості формування цифрового підпису, пропонується замість модулярної арифметики використовувати поліноміальну арифметику полів Галуа, в якій такі базові операції, як експоненціювання і множення, потребують значно менших обсягів обчислень ніж у класичній модулярній арифметиці. Так, піднесення числа до квадрату зводиться до операції вставки нулів між розрядами числа, а відсутність переносів, в свою чергу, зменшує обчислювальну складність операцій множення і додавання. Важливою особливістю операцій на скінчених полях є незалежна обробка розрядів, що дає змогу ефективно організувати розпаралелювання обчислювального процесу.

Пропонується метод формування цифрового підпису, що базується на використанні циклічних властивостей операції експоненціювання на полях Галуа та знання періоду повторення певних чисел в полях Галуа, якщо відомі поліноми, на які розкладається породжуючий поліном поля.

Циклічні властивості операції експоненціювання чисел в полях Галуа були досліджені в [1].

Нехай дано поле *GF(M(x))*. Для будь-якого числа *A*, що співвідноситься з поліномом *a(x)* з поля *GF(M(x))*, існує таке найменше ціле додатне *T*, що$A|^T remM = A$. Число*T* називається періодом повторення або порядком числа *A*. Числа, що належать до одного поля і мають однаковий період називаються такими, що належать до однієї циклічної групи.

Нехай дано два простих поліноми *g(x)* і *p(x)*, ступенів відповідно *d* і *v*. Нехай існують $h = 2^d-1$, $l = 2^v-1$. Тодіh іlможна представити добутком простих множників відповідно як $h = \alpha_1^{k1} \alpha_2^{k2} \dots \alpha_n^{kn}$і$l = \beta_1^{z1} \beta_2^{z2} \dots \beta_m^{zm}$. Числа в полі, породженому добутком *g(x)* і *p(x)*, мають періоди повторення, значення яких відповідають усім можливим комбінаціям добутків простих множниківg(x) і p(x) і їх степенів. Кількість періодичних груп обчислюється за формулами комбінаторики для сполучень з *n* елементів по *m*. При кількості простих множників у степенях ≤ 3 (наприклад, якщо канонічний розклад *g* і *p* виглядає так: 5^2, 7^2, 11^3, 31) кількість груп чисел, що мають однаковий період можна обчислити за формулою: ф

$$S = \sum_{m=1}^{n} C_m^n + (\sum_{i=1}^{p} k_i - p) \sum_{m=1}^{n-1} C_m^{n-1} + (C_2^{\sum k_i - p} - \sum_{i=1}^{p} k_i - (p+1)) + \\ + \prod_{i=1}^{p} (k_i - 1) \sum_{m=1}^{n-p} C_m^{n-p} + \sum_{i=1}^{p} (k_i - 1)$$

Наприклад, якщо в якості *g(x)* і *p(x)* взяти 11 і 55 та обчислити породжуючий поліном поля *M(x)* = *p(x)*⊗*g*(*x*), числа будуть згруповані за наступними періодами: 1, 7, 31, 217.

Група чисел з періодом T = 1 містить наступні числа: 1,*a* = *u*⊗*p*та*b* = *w*⊗*g* такі, що *a*⊕*b* = *1*.

Згідно з [2], $(u \otimes p)|^{h+1} remm = u \otimes p$.

Якщо *h* та *l* - прості числа, то групи чисел з періодами *T* = *h*+*1* або*T* = *l*+*1* містять добутки $\varphi_1 \otimes p$, $\varphi_2 \otimes p$, ... $\varphi_{h-1} \otimes p$та $\eta_1 \otimes g$, $\eta_2 \otimes g$ ... $\eta_{l-1} \otimes g$відповідно.

В групі чисел з *T* =*h*· *l* знаходяться усі інші числа.

Базуючись на вказаних вище властивостях, було розроблено метод цифрового підпису, що передбачає використання періоду повторення чисел поля як закритого ключа.

З написаного вище стає очевидним, що період повторення чисел в полі Галуа визначається множниками породжуючого полінома *M(x)*, які є відомими лише відправнику. Для зловмисника обчислення періоду числа з поля *GF(M(x))* шляхом простого експоненціювання виявилося б занадто ресурсомістким, приймаючи до уваги, що в реальній практиці розрядності операндів становлять 2048 та 4096. З цієї причини в методі цифрового підпису було б доцільним використовувати період *T* в якості закритого ключа.

Для методу, що пропонується, інтерес представляють лише числа з періодом *T* = *h*· *l*. Пошук числа *A*, що належить до цієї групи виконується наступним чином. Вибирається випадкове число $1 < A < 2^{dv} - 1$, що задовольняє наступним умовам:

1. *A remg≠ 0*
2. *A remg≠ 1* (1)

3. $A\ remp \neq 0$

4. $A\ remp \neq 1$

Якщо всі умови виконані, можна вважати, що число A не належить до перших трьох груп, а значить належить до останньої групи з $T = h \cdot l$. Якщо умови не виконані вибирається нове випадкове число число.

Процедура формування цифрового підпису виглядає наступним чином:

1. Відправник обчислює хеш-функцію документа m як $H(m)$, що в двійковому представленні має розрядність l. При використанні алгоритму SHA256, $l = 256$.

2. Відправник довільнимчином вибирає пару простих поліномів $p(x)$ та $g(x)$ з різними степенями: $p(x) = x^v + p_{v-1} \cdot x^v + ... + + p_1 \cdot x + p_0$ степені v та $g(x) = x^d + g_{d-1} \cdot x^{d-1} + + ... + g_1 \cdot x + g_0$ степені d, де $p_0, p_1, ..., p_{v-1} \in \{0,1\}$, $g_0, g_1, ..., g_{d-1} \in \{0,1\}$, причому $d > v$ і $(d + v) > 258$.

3. Відправник формує поліном $M(x)$ у вигляді поліноміального добутку вибраних двох поліномів $p(x)$та $g(x)$: $M(x) = p(x) \otimes g(x)$.

4. Відправник вибирає число A, що задовольняє умові (1) і співвідноситься з поліномом $a(x)$ в полі та період повторення якого відомий тільки відправнику і становить T. $T > 2^{257}$.

5. Відправник вибирає випадкове число e таке, що $1 < e < 2^{dl}$.

6. Відправникобчислює число d, що є мультиплікативно оберненим до e, тобто для якого виконується рівність $d \otimes e\ remM = 1$.Число d становить відкритий ключ. Якщо такого числа не існує, відправник повертається до пункту 5.

7. Відправник вибирає випадкове число k: $0 < k < 2^{255}$і обчислює $r = T - H(m) - k$. Далі відправник обчислює $F = A|^k \otimes A|^r remM$.

8. Відправник обчислює$W = F \otimes e\ remM$і додає отримане число до цифрового підпису. Цифровий підпис становлять наступні числа: $<W, A, M, d>$.

Запропонована процедура перевірки цифрового підпису отримувачем:

1. Отримувач отримує документ m.

2. Отримувач обчислює хеш-функцію документа m як $H(m)$.

3. Отримувач обчислює $C = A|^{H(m)} remM$.

4. Отримувач обчислює$D = W \otimes d \otimes Crem M$. Якщо $D = A$, то вважається, що верифікація пройшла успішно і підпис вірний.

Аналіз ефективності. Як і для будь-якого механізму криптографічного захисту даних, ефективність запропонованого методу ідентифікації віддалених користувачів оцінюється за двома базовими критеріями: рівнем захисту та часовими характеристиками реалізації.

Оцінку рівня захищеності доцільно виконувати з позиції третьої сторони, яка може мати доступ до документу та цифрового підпису, але не знає множників, на які розкладається утворюючий поліном $M(x)$ поля Галуа.

Для зловмисника, що має доступ до каналу передачі даних, задача відтворення періоду числа A зводиться до задачі розкладання відомого поліному $M(x)$ на два простих множника $p(x)$ та $g(x)$ з різними ступенями. Вирішення такої задачі шляхом перебору для реальних степенів поліномів виходить далеко на межі технічних можливостей сучасних комп'ютерних систем.

Основна перевага запропонованого способу формування цифрового підпису полягає в тому, що використання експоненціювання в полях Галуа на

відміну від модулярного експоненціювання дозволяє значно прискорити час виконання програм та спростити апаратну реалізацію. Нижче наведені основні чинники, які дозволяють прискорити програмну реалізацію незворотних перетворень на полях Галуа в порівнянні з мультиплікативними перетвореннями модулярної арифметики, що лежать в основі існуючих методів:

- операція піднесення числа до квадрату, питома вага якої складає 75% об'єму обчислень, на полях Галуа зводиться до вставки нулів між бітами числа, тобто не потребує ніяких обчислювальних операцій. В той же час операція піднесення до квадрату n-розрядного числа в традиційній алгебрі потребує виконання $(\frac{n}{m})^2/2$ операцій процесорного множення;

- при виконанні операцій на полях Галуа кожен розряд оброблюється незалежно від інших: це дає змогу ефективно організувати розпаралелювання обчислювального процесу, особливо при використанні апаратних засобів;

- операції на полях Галуа не використовують переносу, що значно прискорює виконання в порівнянні з традиційною алгеброю, для яких формування міжрозрядних переносів для розрядностей 2018 і 4096, що здебільшого використовуються на практиці, потребує помітних затрат часових та апаратних ресурсів.

В роботі [1] показано, що експоненціювання в полях Галуа виконується на 2-3 порядки швидше у порівнянні з модулярним експоненціюванням, яке є базовою процедурою для існуючих методів DSA [4], RSA [4] та Ель-Гамаля[4] реалізації цифрового підпису.

Експериментальні дослідження показали, що при апаратній реалізації алгоритму на програмованих матрицях досягається значне прискорення процедур формування цифрового підпису в порівнянні з методом Ель-Гамаля. Зокрема, моделювання засобами VHDL показало зростання швидкості формування цифрового підпису на 1-2 порядки.

Висновки. В роботі досліджено можливості використання незворотних перетворень на полях Галуа для створення ефективних механізмів формування цифрового підпису. Зокрема, теоретично досліджені властивості циклічності операції експоненціювання на полях Галуа спеціальних класів.

На основі отриманих теоретичних результатів запропоновано метод формування цифрового підпису.

Внаслідок того, що ці операції виконуються на 1-2 порядки швидше за мультиплікативні операції модулярної арифметики, що лежать в основі відомих методів контролю цілісності та автентичності даних, використання запропонованого методу дозволяє суттєво прискорити процес формування цифрового підпису.

Список літератури

1. Николайчук Я. Коди поля Галуа: теорія та застосування./Монографія/ Николайчук Я. - Тернопіль: ТзОВ "Терно граф". - 2012. – С. 392.

2. Марковський О. Використання алгебри полів Галуа для реалізації концепції «нульових знань» при ідентифікації та автентифікації віддалених користувачів. / Марковський О., Захаріудакіс Лефтеріс, Максимук В. - Електронне моделювання. - 2017. - Т.39. - № 6. - С. 32 – 46.

3. BonehD. TwentyYearsofAttacksontheRSACryptosystem./ BonehD. - NoticesoftheAmericanMathematicalSociety (AMS). – 1999. - Vol. 46. - No. 2. - PP. 203-213.

4. Schneier B. Applied Cryptography. Protocols. Algorithms and Source codes in C./ Schneier B. - Ed.John Wiley. – 1996. – P. 784.

5. Rivest R.L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems./ Rivest R.L., Shamir A., Adleman L. - Computers and Mathematics with Applications. - 1979.– Vol. 5. – No. 3. - PP. 169-178.

6. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms./ ElGamal T.A. - IEEE Trans Inf Theory. – 1985. – Vol. 31. – No. 3. - PP. 469–472.

ДОВІДКА ПРО АВТОРІВ

Марковський Олександр Петрович – доцент, кандидат технічних наук, кафедра обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Markovskyi Oleksandr – associate professor, candidate of engineering sciences, Department of Computer Engineering, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”.

E-mail: markovskyy@i.ua

Сербін Олександр Дмитрович – студент, кафедра обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Serbin Oleksandr – student, Department of Computer Engineering, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”.

E-mail: s0meparry@gmail.com

O. Markovskyi, O. Serbin

A DIGITAL SIGNATURE ALGORITHM BASED ON POLINOMIAL ARIFMETICS OF GALOIS FIELDS

Relevance of the topic. In many spheres of human activity, in particular in the banking sector, there is a transition from the paper form of documents to digital, which greatly increases the efficiency of their processing. A prerequisite for the qualitative interaction of the parties with the participation of digital documents is the application of effective mechanisms for controlling their integrity and authorship. A key role among these mechanisms is taken by the schemes for the formation and verification of digital signatures.

Target setting. With the advent and development of cloud technologies, a wide range of users gain access to large volumes of computing resources that can be exploited by malicious people to break the existing algorithms of digital signature. The potential of cloud technologies indirectly affects the reduction of cryptographic stability of existing algorithms and violates the balance of power in the world of information security; this requires finding adequate solutions for improving existing cryptographic methods, including digital signature technology.

Actual scientific researches and issues analysis. Since the first publication of the digital signature algorithm, many options have been developed. The most commonly used algorithms are based on RSA, El Gamal and DSA. They are also the most researched and are considered to be cryptographic resistant. These algorithms are widely used and adopted as state standards in many countries around the world.

Uninvestigated parts of general matters defining. With the passage of time and the advancement of computer technology, the need to improve the level of security of algorithms is also increasing. The level of security for this class of algorithms can only be improved by increasing the length of the operands. This leads to exponential growth of computing complexity and, in turn, to significant increase in the implementation time, that violates the time standards of network protection protocols.

The research objective. The objective is to increase the speed of the formation of a digital signature by using an alternative mathematical basis - finite Galois fields.

The statement of basic materials. A digital signature scheme is proposed, which is based on the use of cyclic properties of the exponential operation in Galois fields and knowledge of the period of repetition of certain numbers in Galois fields, if known polynomials on which the generating polynomial of a field is decomposed. The main advantage of the proposed scheme of a digital signature is that the use of exponentiation in the fields of Galois, in contrast to the modular exponentiation, can significantly accelerate the execution time of the programs and simplify the hardware implementation.

Conclusion. The possibilities of using irreversible transformations in Galois fields to create effective mechanisms for the formation of a digital signature are explored. Based on the obtained theoretical results the method of digital signature creation is proposed. Due to the fact that these operations are performed 1-2 orders faster than multiplicative operations of modular arithmetic, which are the basis of known methods for controlling the integrity and authenticity of data, the use of the proposed method allows to significantly accelerate the process of forming a digital signature.

Key words: digital signature, Galois fields, data protection, irreversible transformations.