УДК 004.056.2

МАРКОВСЬКИЙ О.П.,
ФЕДОРЕЧКО О.І.,
САЇДРЕЗА МАХМАЛІ

ТЕХНОЛОГІЯ ЦИФРОВОГО ПІДПИСУ DSA НА ОСНОВІ АРИФМЕТИКИ ПОЛІВ ГАЛУА

Запропоновано модифікацію алгоритму формування цифрового підпису DSA, що базується на новому використанні арифметики кінцевих полів. Наведено математичне обґрунтування запропонованого підходу. Описано технології генерації ключів, формування цифрового підпису та його перевірки. Для всіх цих процедур наведено числові приклади. Доведено, що використання арифметики кінцевих полів дозволяє помітно прискорити роботу з цифровим підписом. Запропонована модифікація алгоритму формування цифрового підпису DSA орієнтована на апаратну реалізацію.

The modification of DSA techniques based on novel application of arithmetic of finite fields are presented. The mathematical background of the proposed approach is first presented. The techniques of public and secret keys generation, forming and verification of signature based of finite fields arithmetic are described. A numerical example for all mentioned procedures is given. It has been showed that using of finite fields arithmetic may greatly accelerate the processing of DSA signatures. The proposed DSA modification is oriented for hardware implementation.

Вступ

Сучасний етап розвитку інформаційних технологій все більше підтверджує відому тезу академіка В.М.Глушкова про настання ери безпаперової звітності. Фактично, вже сьогодні зростаючий рівень динаміки ділових відносин диктує такий рівень оперативності документообігу, що може бути досягнутим лише використанням сучасних комп'ютерних та мережових технологій. Особливо рельєфно ця тенденція виявляється в банківській справі. За умов переходу до безпаперового документообігу великої ваги набуває забезпечення автентичності документів: тобто має гарантуватися авторство документу, а також те, що при передачі по відкритим мережам його не змінено.

Для забезпечення цілісності та автентичності документів з середини 80-х років активно використовуються криптографічні механізми цифрового підпису. В середині 90-х в більшості країн було прийнято криптографічні стандарти цифрового підпису. Всі вони базуються на математичних операціях модулярного експоненціювання над числами великої розрядності. Відповідно, обчислювальна реалізація існуючих механізмів цифрового підпису потребує помітних витрат часу. Зростання обчислювальних потужностей, які потенційно можуть бути використані зловмисниками для підробки цифрового підпису диктує необхідність постійного збільшення розрядності чисел, що застосовуються при формуванні цифрового підпису. Так, в сучасних умовах для забезпечення потрібного рівня захищеності, розрядність чисел становить 2048 з перспективою збільшення в найближчі роки до 4096. При реалізації операцій модулярного експоненціювання збільшення розрядності чисел має наслідком експоненційне зростання часу обчислень. Причому, темпи зростання об'єму обчислень випереджають збільшення швидкодії комп'ютерних систем. Особливо гостро проблема часу формування цифрового підпису стоїть для термінальних портативних малопотужних обчислювальних пристроїв, які підтримують мережові протоколи захисту інформації.

Таким чином, проблема зменшення обчислювальної складності процесів формування цифрового підпису і, відповідно, прискорення контролю автентичності документів є на сьогоднішній день актуальною.

Аналіз існуючих алгоритмів цифрового підпису

Цифровий підпис інформаційного повідомлення – це криптографічний механізм, який гарантує по-перше, цілісність – тобто те, що повідомлення не зазнало змін, а по-друге: авторство, тобто те, що повідомлення підписано певним автором [1].

Початок практичному використанню цифрового підпису банківськими установами було

покладено створенням механізмів несиметричної криптографії. Перші механізми цифрового підпису мали за основу відомий алгоритм несиметричного шифрування RSA. Згодом стало зрозумілим, що використання алгоритмів несиметричного шифрування неефективне, оскільки пов'язане зі надлишковими витратами обчислювальних ресурсів. Розпочалися роботи зі створення ефективних спеціалізованих механізмів цифрового підпису. Етапним стало прийняття в серпні 1991 року стандарту цифрового підпису DSS (Digital Signature Standard). Цей стандарт передбачає процедуру перевірки авторства та цілісності повідомлення згідно з алгоритмом DSA (Digital Signature Algorithm) [2]. Згодом, в Росії було прийнято в якості стандарту практично ідентичний за математичними принципами алгоритм формування цифрового підпису ГОСТ Р.34.10-94 [1].

Сутність алгоритму DSA полягає в слідуючому. При генерації ключів алгоритму виконується наступна послідовність дій.

1) Генерується просте l-розрядне число p. Наприклад, при l=6 p= 43 = 101011_2.

2) Знаходиться число q фіксованої розрядності $b \approx l/2$, що є подільником числа p-1. Наприклад, якщо p= 43, то p-1= 42 = 6·7 і тоді q=7, b=3.

3) Довільним чином вибирається число h, таке, що $h<p$-1 і $h^{(p-1)/q} \bmod p > 1$. Наприклад, якщо вибрати h = 5, то $5^6 \bmod 43 = 16$.

4) Обчислюється $g = h^{(p-1)/q} \bmod p$. Наприклад при p=43, q=7 та h=5 g=16.

5) Вибирається число $x<q$, наприклад, x = 5.

6) Обчислюється $y = g^x \bmod p$. В рамках поточного прикладу $y=16^5 \bmod 43 = 21$.

Згенеровані описаним способом числа p, q g та y – являються компонентами відкритого ключа, а x – закритий ключ.

Процедура формування цифрового підпису лицем, що знає закритий ключ x полягає в наступному.

При передачі документу m формується його хеш-сигнатура $H(m)$ фіксованої розрядності. Стандартом для формування передбачено використання хеш-алгоритму SHA-1 [3]. Нехай, для прикладу, $H(m)$=37. Лице, що підписує повідомлення виконує таку послідовність дій:

1) Довільним чином вибирається k таке, що $k<q$; наприклад k = 3.

2) Обчислює $r = (g^k \bmod p) \bmod q$. В рамках прикладу, що розглядається, значення r обчислюється як: $r = (16^3 \bmod 43) \bmod 7 = 11 \bmod 7 = 4$.

3) Визначається мультиплікативна інверсія k^{-1} так, що $k \cdot k^{-1} \bmod q = 1$. Для приклада, при k = 3 значення k^{-1}= 5, оскільки 3·5 mod 7 =15 mod 7 =1.

4) Обчислюється $s = (k^{-1} \cdot (H(m) + x \cdot r) \bmod q$. В рамках прикладу, що розглядається значення s =(5·(37+5·4))mod 7 = 285 mod 7 = 5.

5) Цифровий підпис, який складається з двох компонентів r та s відсилається приймачеві.

Одержувач документу проводить перевірку цифрового підпису наступним чином.

1) Для отриманого документу m' за встановленим хеш-алгоритмом обчислюється хеш-сигнатура $H(m')$. Якщо документ не змінено, то $m=m'$ і відповідно $H(m)=H(m')$. Наприклад, якщо $H(m)$=37 і документ не змінено при передачі, то $H(m')$ =37.

2) Знаходиться мультиплікативна інверсія s^{-1} така, що $s \cdot s^{-1} \bmod q = 1$. Якщо q=7 і s=5 тоs^{-1}=3.

3) Обчислюється $u_1 = (H(m') \cdot s^{-1}) \bmod q$. Для прикладу, що розглядається $u_1 = (37 \cdot 3) \bmod 7 = 111 \bmod 7 = 6$.

4) Обчислюється $u_2 = (r \cdot s^{-1}) \bmod q$, зокрема для прикладу $u_2 = (4 \cdot 3) \bmod 7 = 12 \bmod 7 = 5$.

5) Обчислює $v = ((g^{u_1} \cdot y^{u_2}) \bmod p) \bmod q$. Для прикладу, що розглядається $v = ((16^6 \cdot 21^5) \bmod 43) \bmod 7 = 11 \bmod 7 = 4$

6) Якщо $v = r$, то вважається, що документ не зазнав змін при передачі і від підписаний лицем, яке знає закритий ключ x.

Математичний сенс процедури DSA полягає в тому, що знаючи x, автор формує $s = (k^{-1} \cdot (H(m) + x \cdot r) \bmod q$. Зрозуміло, що $(s \cdot k) \bmod q = (k \cdot k^{-1} \cdot (H(m)+x \cdot r)) \bmod q = (H(m)+x \cdot r) \bmod q$. Якщо $H(m)=H(m')$, то $H(m')+x \cdot r = s \cdot k$. З урахуванням наведеного, за умови того, що прийнятий документ є автентичним справедливо:

$$v = ((g^{u_1} \cdot y^{u_2}) \bmod p) \bmod q =$$

$$= ((g^{H(m') \cdot s^{-1}} \cdot (g^x)^{r \cdot s^{-1}}) \bmod p) \bmod q =$$

$$= (g^{s^{-1} \cdot (H(m')+x \cdot r)} \bmod p) \bmod q =$$

$$= (g^{s^{-1} \cdot k \cdot s} \bmod p) \bmod q = (g^k \bmod p) \bmod q = r$$

Якщо $H(m) \neq H(m')$, то $H(m')+x \cdot r \neq s \cdot k$, і, відповідно, $v \neq r$. Якщо підпис документу зробила інша особа з використанням ключа $x' \neq x$, то $y \neq g^{x'}$ і $v \neq r$. Якщо припустити, що підпис перехоплений зловмисником, то його ціллю є змінити текст документу на $m'' \neq m$ та підібрати таке $x'' \neq x$ щоб $(k^{-1} \cdot (H(m'') + x'' \cdot r) \bmod q = s$. Це зробити важно, так як значення k не передається і, від-

повідно, зловмиснику не відоме. Фактично, потрібно підбирати два b-розрядні числа x'' так, що якщо вважати, що $b \approx l/2$, то об'єм перебору становить 2^l.

Очевидним недоліком DSA є значна обчислювальна складність. В процесі формування цифрового підпису виконується одна операція модулярного експоненціювання b-розрядних чисел, віднаходження мультиплікативної b-розрядної інверсії k^{-1}

Для зменшення обчислювальної складності віднаходження мільтиплікативної інверсії в алгоритмі DSA застосовано зменшення вдвічі розрядності при виконанні цієї операції, оскільки розрядність q приблизно в два рази менша розрядності p.

Для зменшення обчислювальної складності операцій молярного експоненціювання найчастіше використовується метод Монтгомері, який дозволяє звести складну в обчислювальному плані операцію модулярної редукції до зсувів. Застосування для зменшення об'єму обчислень результатів передобчислень неефективне в силу того, що код експоненти змінюється при кожному формуванні цифрового підпису.

Ціллю досліджень є підвищення продуктивності формування та перевірки цифрового підпису.

Алгоритм цифрового підпису на основі експоненціювання на полях Галуа

Операція модулярного експоненціювання над числами, довжина яких значно перевищує розрядність процесора, виконується фрагментами. При виконанні арифметичної операції над кожним із фрагментів потрібно враховувати можливість переносу в наступний фрагмент. Виходячи з цього, одним з напрямків підвищення продуктивності реалізації модулярного експоненціювання є заміна арифметичних операцій на логічні, при виконання яких не потрібно враховувати перенос. Фактично мова йде при заміну операції арифметичного модулярного експоненціювання на аналогічну операцію на полях Галуа.

В плані захищеності використання операцій арифметичного модулярного експоненціювання та експоненціювання на полях Галуа практично є ідентичним. Дійсно, при використанні модулярного експоненціювання $A^h \bmod M = \xi$ порушення захисту в математичному сенсі є ідентичним віднаходженню мінімального h з рівняння $A^h = j \cdot M + \xi$ при відомих значеннях A, M та ξ і не відомому значенні j. Практично це рівняння може бути розв'язане лише шляхом перебору, об'єм якого при великій розрядності перевищує технічні можливості комп'ютерних систем. Якщо через символ $\otimes$ позначити операцію множення без переносів, через $A|^p$ – експоненту степені p на основі множення без переносів, тобто $A|^h = \overset{h}{\underset{j=1}{\otimes}} A$, а через $D \operatorname{rem} M$ – остачу від поліноміального ділення D на M, то операція експоненціювання на полі Галуа з утворюючим поліномом M може бути позначена як $A|^h \operatorname{rem} M$. При застосуванні експоненціювання на полях Галуа для захисту даних, його порушення в математичному сенсі означає віднаходження мінімального h, що задовольняє рівнянню $A|^h = j \otimes M \oplus \xi$ в якому заданими є значення A, M та ξ. Цілком очевидним є те, що єдиним шляхом розв'язання цього рівняння є також перебір.

Аналіз математичних принципів, покладених в основу DSA показує, що в ньому використовується два простих числа p і q, для яких існує g таке, що:

$$g^q \bmod p = 1. \qquad (1)$$

Відповідно, за умови (1) для будь-яких цілих x та n виконується $(g^{x+n \cdot q} \bmod p) \bmod q = (g^x \bmod p) \bmod q$.

Аналогічно, в модифікації DSA на основі експоненціювання на полях Галуа потрібно також застосування 3-х компонент: l-розрядного числа p, b-розрядного числа q та числа g для яких (1) трансформується в:

$$g|^q \operatorname{rem} p = 1. \qquad (2)$$

Число p є простим в алгебрі множення без переносів, тобто його не можна представити у вигляді добутку без переносів двох чисел. Прикладом 9-розрядного (l=9) простого в алгебрі множення без переносів є число $p=299_{10} = 100101011_2$. Число q має бути простим в арифметичному сенсі подільником $2^{l-1}-1$. Наприклад, якщо l=9, то $2^{l-1}-1 = 255 = 3 \cdot 5 \cdot 17$, відповідно, можливим варіантом може бути q=17. Умові (2) задовольняє g=29.

Процес генерації ключів модифікації DSA на основі експоненціювання на полях Галуа полягає в наступному:

1) Генерується просте в алгебрі множення без переносів l-розрядне число p. На практиці число l має бути не меншим 1025. Наприклад, вибирається 9-розрядне число p=299.

2) Знаходиться число q – один із простих, в арифметичному сенсі, подільників числа 2^{l-1}-1 та число g, що задовольняє (2). Якщо p=299, то можливими значеннями q та g є q=17 і g=29.

3) Вибирається випадкове x, наприклад x=10.

4) Обчислюється x=10 = $g|^x$ rem p. Якщо p=299, g=29, а x=10, то $y = 29|^{10}$ rem 299 = 114.

Згенеровані описаним способом числа p, q g та y – являють собою відкритий ключ, тоді як x – закритий ключ.

Процедура формування цифрового підпису лицем, що знає закритий ключ x полягає в наступному.

При передачі документу m формується його хеш-сигнатура $H(m)$ фіксованої розрядності. Нехай, для прикладу, $H(m)$=134. Лице, що підписує повідомлення виконує таку послідовність дій:

1) Довільним чином вибирається k таке, що $k<q$; наприклад k = 14.

2) Обчислюється $r = (g|^k$ rem $p)$ mod q. Якщо p=299, g =29, q=17, а k=14, то $y = (29|^{14}$ rem 299)mod 17 = 88 mod 17 = 3.

3) Визначається мультиплікативна інверсія k^{-1} така, що $k \cdot k^{-1}$ mod q = 1. При q=17 і k =14 значення k^{-1} = 11, оскільки 11·14 mod 17 = 154 mod 17 =1.

4) Обчислюється $s = (k^{-1} \cdot (H(m) + x \cdot r) \bmod q$. В рамках прикладу, що розглядається значення s =(11·(134 + 10·3)) mod 17 = 1804 mod 17 = 2.

5) Цифровий підпис, який складається з двох компонентів r та s відсилається одержувачу документу. Для наведеного вище прикладу одержувачу відсилається пара r =3 і s =2.

Одержувач документу отримує текст документу m' та дві компоненти цифрового підпису (r та s). Перевірка цифрового підпису проводиться виконанням наступної послідовності дій:

1) За допомогою встановленого хеш-алгоритму обчислюється хеш-сигнатура прийнятого документу $H(m')$.

2) Обчислюється мультиплікативна інверсія s^{-1} компоненти s цифрового підпису, тобто знаходиться таке s^{-1}, що добуток $s \cdot s^{-1}$ mod q = 1. Для s=2 s^{-1} = 9 оскільки 18 mod 17 = 1.

3) Обчислюється $u_1 = (H(m') \cdot s^{-1}) \bmod q$. Для прикладу, що розглядається u_1 = (134·9) mod 17 = 1206 rem 17 = 16.

4) Обчислюється $u_2 = (r \cdot s^{-1}) \bmod q$. Для поточного прикладу u_2 = (3·9) mod 17=27 mod 17 =10.

5) Обчислюється $v = ((g|^{u_1} \otimes y|^{u_2})$ rem $p)$mod q. Для прикладу, що розглядається, чисельне значення v=((29|^{16}⊗114|^{10}) rem 299) mod 17 = ((51⊗130)rem299)mod 17=(6630rem 299)mod17= = 88 mod 17 = 3.

6) Якщо $v = r$, то вважається, що документ не зазнав змін при передачі, а також він підписаний лицем, яке знає закритий ключ x. Для прикладу, що ілюструє виклад, v=3=r, тобто цілісність та автентичність документу вважається доведеною.

Оцінка ефективності

Головною перевагою запропонованого способу формування та перевірки цифрового підпису на основі експоненціювання на полях Галуа є менша обчислювальна та часова складність у порівнянні з модулярним експоненціюванням, що використовується в стандарті DSA.

Базовою операцією формування та перевірки цифрового підпису є модулярне експоненціювання, тобто обчислення $a|^E$ rem p, де a та p - суть l-розрядні числа, а E являє собою b-розрядне число. За класичним алгоритмом експоненціювання, ця операція включає в себе b циклів, по числу розрядів експоненти, в кожному з яких виконується, в середньому, 1.5 операцій множення l-розрядних чисел.

В свою чергу, кожна операція множення складається з власне операції множення та редукції. При модулярному множенні редукція полягає в віднаходженні залишку від арифметичного ділення коду добутку на модуль, а при множенні на полі Галуа редукція полягає в обчисленні залишку поліноміального ділення добутку на утворюючий поліном поля Галуа.

Якщо вважати що всі розряди множника дорівнюють одиниці, то формування молодшого розряду добутку не потребує арифметичних операцій, для обчислення другого розряду потрібно виконати одну операцію додавання. Для формування третього розряду потрібно реалізувати дві операції додавання та, зі ймовірністю 0.5, ще одну операцію додавання переносу. При цьому середня кількість переносів в наступний розряд, четвертий розряд, становить 1.25. Узагальнюючи, можна говорити, що формування i-го розряду добутку ($i \le l$) потребує i-1 бітових операцій додавання та, в середньому, $\xi(i) = \sum_{j=2\ldots i} 0.5^{j-1} \cdot (i - j)$ додавань, для врахування переносів. Аналогічно, формування m-го ро-

зряду добутку ($l<m<2\cdot l$) потребує $2\cdot l-m$ бітових операцій додавання та, в середньому, $\xi(2\cdot l-m)$ додавань, для врахування переносів. В цілому, приймаючи до уваги, що лише половина розрядів множника, в середньому, дорівнює одиниці, сумарна кількість D_a бітових при виконанні арифметичного множення становить:

$$D_a = \sum_{i=2}^{l} ((i-1) + \xi(i)) \approx l^2. \qquad (3)$$

При виконанні множення без переносів середня кількість D_g бітових операцій додавання становить:

$$D_g = \sum_{i=2}^{l} (i-1) \approx \frac{l^2}{2}. \qquad (4)$$

Порівняння формул (2) та (3) показує, що обчислювальна складність множення без переносів практично вдвічі менша арифметичного множення. Аналогічний аналіз проведений щодо складності редукції показує, що арифметична редукція має вдвічі більше обчислювальну складність у порівнянні з віднаходженням залишку поліноміального ділення.

Таким чином, перехід від традиційної арифметики до арифметики на кінцевих полях при виконанні базових для технологій цифрового підпису операцій модулярного експоненціювання дозволяє вдвічі зменшити обчислювальну складність.

Суттєво більший виграш досягається при порівнянні часової складності. Як було показано вище, кількість операцій додавання l-розрядних слів при арифметичному множенні та множенні на полях практично однакова. Проте, кожен із розрядів при додаванні на полях оброблюється незалежно, в той час, як при виконанні арифметичного додавання потрібно формувати перенос.

При використанні найбільш швидкодіючих схем прискореного переносу довжина критичного шляху його формування становить $1.5\cdot\log_2 l$. Це означає часова складність формування цифрового підпису з використанням арифметики полів Галуа не менш як в $1.5\cdot\log_2 l$ разів менша ніж при застосуванні традиційної арифметики. Враховуючи, що на практиці $l\geq 1024$, виграш у часовій складності становить не менше 15 разів.

В роботі [4] запропоновано ефективний спосіб обчислення експоненти на полях Галуа непрямим шляхом, який з використанням таблиць передобчислень дозволяє на порядки прискорити виконання цієї операції.

З викладеного зрозуміло, що повною мірою переваги запропонованої модифікації DSA з використанням арифметики кінцевих полів можуть бути реалізовані в рамках апаратного виконання.

Висновки

Для підвищення продуктивності формування та перевірки цифрового підпису DSA запропонована його модифікація. Модифікація полягає в використанні при реалізації найбільш ресурсоємкої операції роботи з цифровим підписом - модулярного експоненціювання арифметики кінцевих полів, зокрема полів Галуа. Розроблено відповідні технології генерування ключів, формування та перевірки цифрового підпису.

Доведено, що використання арифметики кінцевих полів замість традиційної дозволяє помітно прискорити роботу з цифровим підписом. Запропонована модифікація алгоритму формування цифрового підпису DSA орієнтована на апаратну реалізацію.

Список літератури

1. ГОСТ Р.34.10-94. Системы обработки информации. Защита криптографическая. Алгоритм формирования цифровой подписи.
2. Digital Signature Standard (DSS).#186. US Department of commerce, National Institute of Standards and Technology, 1994.
3. Secure Hash Standard. Federal Information Processing Standard Publication #180, US Department of Commerce, National Institute of standard and technology, 1995.
4. Самофалов К.Г. Марковський О.П., Шаршаков А.С. Способ ускоренной реализации экспоненцирования на полях Галуа в системах защиты информации // Проблеми інформатизації та управління. Збірник наукових праць: Випуск 2(33).-К.,НАУ.- 2011.- С.143-151.