УДК 004.056.53

О.П. Марковський, І.В. Ткач, Д.Г. Іванов

Національний технічний університет України "КПІ", Київ

ОДИН ПІДХІД ДО ПРИСКОРЕННЯ СТРОГОЇ ІДЕНТИФІКАЦІЇ ВІДДАЛЕНИХ АБОНЕНТІВ

В статті пропонується підхід до прискорення основаної на криптографічно строгій концепції "нульового розголошення" ідентифікації віддалених абонентів. Запропонований підхід має за основу використання більш простої, з точки зору обчислювальної реалізації, арифметики кінцевих полів замість модулярної арифметики. Теоретично обґрунтовано і розроблено модифікації класичних схем строгої ідентифікації абонентів з використанням запропонованого підходу. Робота модифікованих схем ідентифікації ілюструється чисельними прикладами. Теоретичне та експериментальне дослідження розроблених схем доводить, що запропонований підхід дозволяє на порядок прискорити програмну реалізацію ідентифікації, основаної на криптографічно строгій концепції "нульового розголошення" і на 2-3 порядки - апаратну.

***Ключові слова**: строга ідентифікація абонентів, концепція нульового розголошення, арифметика кінцевих полів, швидке експоненціювання на кінцевих полях.*

Вступ

На початку 21-го століття інформаційна інтеграція виступає найбільш дієвим чинником технологічного прогресу в усіх областях людської діяльності, включаючи військову. Швидкий прогрес комп'ютерних технологій стимулює динамічне розширення використання в військові області багато абонентських розподілених систем, що виконують функції збору і обробки інформації, прийняття рішень та неперервного управління. Успішність практичного використання таких систем значною мірою визначається ефективністю ідентифікації їх абонентів. Аналіз протиборства в сфері інформаційних технологій під час воєнних конфліктів останніх років переконливо свідчить про те, що підсистеми ідентифікації абонентів розподілених систем управління військовими діями найчастіше стають об'єктами атак.

Добре відомо, що найбільш надійними є схеми ідентифікації, в основі яких лежить криптографічно строга концепція нульового розголошення, яка реалізує принципи єдиного власника секретної інформації та одноразовості паролів доступу до даних. Практичне використання таких прогресивних схем ідентифікації значною мірою обмежується тим, що їх практична реалізація вимагає значних обчислювальних ресурсів. Це пов'язано з тим, що існуючі схеми строгої ідентифікації базуються на використанні складних операцій модулярного експоненціювання, що виконуються над числами розрядністю 1024-2048 з перспективою зростання до 4096 уже в найближчі роки. При реалізації операцій модулярного експоненціювання збільшення розрядності має наслідком експоненційне зростання об'єму обчислень. При цьому темпи збільшення об'єму обчислень суттєво випереджають зростання продуктивності комп'ютерних систем. Особливо гостро проблема швидкої реалізації ідентифікації на основі концепції "нульового розголошення" стоїть для портативних вбудованих мікроконтролерів з обмеженою продуктивністю та енергоспоживанням, які для військових застосувань, часто виступають в якості термінальних пристроїв абонентів [1].

Таким чином, проблема прискорення обчислювальної реалізації основаної на криптографічно строгій концепції "нульового розголошення" ідентифікації віддалених абонентів багатокористувацьких систем управління є актуальною для сучасного етапу розвитку інформаційних технологій.

Схеми ідентифікації на основі концепції "нульового розголошення"

В сучасних умовах відбувається розширення можливостей для несанкціонованого доступу до закритих інформаційних ресурсів інтегрованих схем за рахунок порушення процедур ідентифікації. Основним чинником цього виступає багатократне зростання обчислювальних потужностей за рахунок використання сучасних технологій розподілених та хмарних обчислень.

Розширення використання в військових застосуваннях бездротових технологій обміну даними розширює можливості втручання в процес ідентифікації. Зокрема, в безпровідних лініях полегшується процедура перехоплення зловмисником пароля легального абонента, а також його заміна після проведения сеансу ідентифікації. Класичним засобом протидії заміні являється періодичне повторне проведення сеансів ідентифікації в процесі взаємодії системи з абонентом. Для цього процедура ідентифікації повинна виконуватися достатньо швидко.

Ще одним шляхом порушення процесів ідентифікації є побічний направлений вплив на роботу системи легальних користувачів, а також шляхом

вірусів або персоналу. Для широкого класу військових багато абонентних систем важливою є виключення можливісті імітації системою звернень до віддаленого користувача.

Якщо враховувати всі вище перелічені обставини, то сучасні засоби ідентифікації абонентів для забезпечення правильного функціонування системи повинні задовольняти наступним вимогам:

1. При ідентифікації службове повідомлення(пароль) повинне змінюватися при кожному зверненні до системи, при цьому всі паролі, що використовуються, повинні бути статично незалежними;

2. Довжина паролю повинна повністю виключати можливість його підбору шляхом перебору;

3. Інформація, яка зберігається в системі не повинна бути достатньою, для відтворення пароля абонента;

4. Процедура ідентифікації повинна виконуватися максимально швидко.

Розрізняють “строгі” та “слабкі” методи ідентифікації. До перших відносяться ті, які задовольняють три перші з вище перелічених вимог. До класу «слабких» належать , наприклад, процедура ідентифікації, що використовується в операційній системі UNIX.

Сама процедура передбачає збереження в системі лише хеш-образів паролів користувачів,проте паролі не змінюються – це дозволяє достатньо просто їх перехоплювати. Сьогодні практично у всіх структурах використовуються “слабкі” методи ідентифікації, проте вони не можуть забезпечувати достатній рівень надійності у системах, де безпека інформації відіграє ключову роль.

До класу “строгих” процедур відносяться методи ідентифікації, в основі яких лежить концепція “нульового розголошення”. Сюди відносяться, зокрема:

схема Шнорра (Schnorr),

схема Гіллоу-Квіскватера (Guillou- Quisquater)

FFSIS (Feige Fiata Shamir Identification Scheme).

FFSIS [2] забезпечує високу надійність процедури ідентифікації. Проте ця схема має свої недоліки, основним з яких є сильне перевантаження ліній передач, так як FFSIS необхідна велика кількість обміну даними в процесі ідентифікації. В випадку, коли є проблеми з перевантаженням ліній передач, більш доцільним є використання алгоритмів Гіллоу-Квіскватера та Шнорра.

Схема ідентифікації з “нульовим розголошенням”, розроблена Л.Гіллоу та Ж.Квіскватером [3], має дещо кращі характеристики ніж вище згадувана схема FFSIS – вона не потребує багатократного повторення циклів акредитації, а також обмін інформацією між системою та абонентом зведений до мінімуму. Проте об’єм необхідних обчислень для цього алгоритму більший ніж для FFSIS.

Генерація ключів в схемі Гіллоу-Квіскватера виконується наступним чином:

Абонент має відкритий пароль J, що на практиці являє собою хеш-сигнатуру символьного рядка імені абонента, нехай $J = 18$. Відкритий ключ системи також включає в себе число n – воно є добутком двох простих чисел p і q. Ці числа зберігаються в таємниці так само як і просте число v. Є рівність $(J \cdot B^v) mod\ n = 1$, у відповідності до якої підбирається секретний ключ B. Наприклад, $p = 31$ і q=29, $p \cdot q = n = 31 \cdot 219 = 899$, $B = 648$ та $v = 19$ так як $(J \cdot B^v) mod\ n = (18 \cdot 648^{19}) \ mod\ 899 = 1$.

Ідентифікації зводиться до наступної послідовності дій:

1. Абонент формує випадкове число r таке, що $1 < r < n - 1$ обчислює значення $T = r^v \ mod\ n$, та відсилає T в систему. Наприклад, нехай $r = 664$, тоді $T = 664^{19} \ mod\ 899 = 765$.

2. Система генерує випадкове d, яке має знаходитися в діапазоні $0 < d < n - 1$, наприклад, $d = 267$. Це значення також пересилається віддаленому абоненту.

3. Абонент обчислює $D = r \cdot B^d \ mod\ n$ та відправляє обчислений код в систему. $D = 664 \cdot 648^{267} \ mod\ 899 = 755$.

4. В системі вираховується

$$T' = D^v \cdot J^d \ mod\ n,$$

якщо $T = T'$, то результат ідентифікації рахується позитивним. Для наведеного прикладу:

$$T' = 755^{19} \cdot 18^{267} mod\ 899 = 765.$$

Схема Шнорра [3] являє собою альтернативу описаним вище схемам FFSIS та Гіллоу-Квіскватера. Надійність схеми базується на складності обчислення дискретного логарифму. Схема Шнорра дозволяє проводити попередні розрахунки, що зручно при незначних обчислювальних ресурсах. Фактично передається лише три повідомлення – це дозволяє зменшити взаємодію в мережах з низькою пропускною здатністю.

Абонент обирає два простих числа p і q, причому останнє повинно бути множником $p - 1$. Наприклад $q = 5$, тоді значення $p - 1$ обчислюється як добуток $q = 5$ на будь-яке парне число: $p - 1 = q \cdot 8 = 40$. Відповідно $p = 41$. Далі необхідно обрати значення a таке, щоб задовольняло умову $a^q mod\ p = 1$. Наприклад, при $a = 10$, виконується $10^5 mod\ 41 = 1$.

Далі вибирається випадкове число $s < q$, наприклад $s = 1$,обчислюється

$-s = q - s = 5 - 1 = 4$. Число s є закритим ключем. Для генерації відкритого ключа потрібно розрахувати $v = a^{-s} \ mod\ p = 37$.

Процедура ідентифікації абонентів зводиться до наступної послідовності дій :

1. Абонент обирає випадкове $r < q$, для прикладу візьмемо $r = 2$, обчислюємо $x = ar \bmod p$, у нашому випадку $x = 10^{2} mod\ 5 = 18$. Потім посилає це число в систему.

2. Система генерує випадкове $e < 2^{t} - 1$ та посилає це значення абоненту. В рамках розглянутого прикладу $t = 6, e = 51$.

3. Наступним кроком для абонента є обчислення значення $y = (r + s \cdot e) \bmod q$ та відправлення його в систему. $y = (2 + 1 \cdot 51) \bmod 5 = 3$.

4. Система перевіряє виконання рівності $x = a^{y} \cdot v^{e} mod\ p$. Для наведеного прикладу ця рівність виконується: $10^{3} \cdot 37^{51} mod\ 41 = 18$. В такому випадку ідентифікація рахується успішною.

Цілком очевидно, що як і для схеми Гіллоу-Квіскватера базовою операцією в схемі Шнорра є модулярне експоненціювання. На практиці, для генерації ключів, зазвичай, використовуються коди великої розрядності(1024). Операція модулярного експоненціювання над числами, довжина яких значно перевищує розрядність процесора, виконується фрагментами.

При програмній реалізації на w–бітному процесорі n-розрядні коди розділяються на s фрагментів ($s = n/w$).

На сьогоднішній день найбільш ефективним алгоритмом модулярного експоненціювання є алгоритм Монтгомері [5], в якому для реалізації редукції використовується не ділення, а зсув. Число операцій процесорного множення при використанні алгоритму експоненціювання Монтгомері дорівнює $3n \cdot s \cdot (s + 1)$, а число операцій арифметичного додавання - $4n \cdot s \cdot (s + 1)$.

Згідно до даних [7] для сучасних процесорів час виконання операції множення $tm \approx 10 \cdot \tau$, а час виконання операції додавання $ta \approx \tau$, де τ- тривалість тактового інтервалу. Тоді час T_M модулярного експоненціювання з використанням алгоритму Монтгомері оцінюється як:

$$T_M = 34 \cdot n \cdot s \cdot (s + 1) \cdot \tau. \qquad (1)$$

Метою дослідження є створення модифікацій схем ідентифікації Шнорра та Гіллоу-Квіскватера, що забезпечують більшу продуктивність програмної та апаратної реалізації в порівнянні з базовими варіантами на основі використання алгебри полів Галуа. Використання в модифікованих варіантах більш простої в обчислювальному плані алгебри кінцевих поліх дозволить зменшити обчислювальну складність процедур ідентифікації, що дозволить прискорити виконання криптографічно “строгої” ідентифікації абонентів при програмній та апаратній реалізаціях.

Модифікація схем ідентифікації Шнорра та Гіллоу-Квіскватера з використанням алгебри полів Галуа

За рахунок використання алгебри без міжрозрядних переносів, можливе значне спрощення обчислень, що пов’язані з реалізацією схем ідентифікації Шнорра та Гіллоу-Квіскватера. Фактично мова йде про заміну арифметичного модулярного експоненціювання на аналогічну операцію на полях Галуа. Переваги використання алгебри полів Галуа стають помітні вже при реалізації її базових обчислювальних операцій: додавання, множення та модулярна редукція – вони виконуються значно швидше в порівнянні з класичними операціями множення, додавання та знаходження остачі від ділення за рахунок відсутності переносів.

Разом з тим, перехід від звичайної алгебри до алгебри кінцевих полів практично не впливає на рівень захищеності схем ідентифікації, оскільки дискретне логарифмування на кінцевих полях, як і звичайне дискретне логарифмування відноситься до класу задач, що не можуть бути розв’язані аналітично [8]. Тому алгебра полів Галуа широко застосовується в алгоритмах захисту інформації, зокрема алгоритмі симетричного шифрування Rijndael та механізмах захисту інформації на основі еліптичних кривих.

В алгебрі полів Галуа операція логічного додавання (XOR) фактично відповідає операції класичного додавання. Якщо через символ ⊗ позначити операцію множення без переносів, через $A|^{q}$ - експоненту степені q,а через $B\ rem\ M$ – остачу від поліноміального ділення B на M, то операція експоненціювання на полі Галуа може бути позначена як $A|^{q}\ rem\ M$.

Сутність запропонованої модифікації схем Шнорра та Гіллоу-Квіскватера в алгебрі полів Галуа полягає в наступному.

В модифікованій схемі Шнорра для генерації ключів обираються два нерозкладних поліноми P(x) та W(x) однакової розрядності, яким відповідають числа p та w. Обчислюється $m = p \otimes w$. Обирається q, що являє собою множник числа $m \ominus 1$ та число a таке, що $a|^{q}\ rem\ m = 1$. Наприклад, можна обрати 5-розрядні числа $p = 17, w = 19$, тоді $m = 291, q = 145, a = 118$.

Обирається випадкове число $s < q$, наприклад $s = 14$,обчислюється $-s = q - s = 131$. Число s є закритим ключем. Для генерації відкритого ключа необхідно розрахувати $v = a|^{-s}\ rem\ m = 118$.

Процедура ідентифікації в модифікованій схемі Шнорра описується такою послідовністю дій:

1. Абонент обирає випадкове $r < q$, для прикладу візьмемо $r = 78$, далі обчислює $x = a|^{r}\ rem\ m$

, для розглянутого прикладу $x = 254$. Це число посилається в систему.

2. Система генерує випадкове $e < 2^t - 1$та посилає це значення абоненту. В рамках розглянутого прикладу $t = 6, e = 5$.

3. Наступним кроком для абонента є обчислення значення $y = (r + s \cdot e)\ mod\ q$ та відправлення його в систему.

$$y = (78 + 14 \cdot 5)\ mod\ 145 = 3.$$

4. Система перевіряє виконання рівності $x = a|^y \cdot v|^e\ rem\ m$. Для приведеного прикладу ця рівність виконується:

$$x = a|^y \cdot v|^e\ rem\ m = 118|^3 \cdot 118|^5\ rem\ 291 = 254.$$

Модифікована схема Гіллоу-Квіскватера працює наступним чином.

Відкритий ключ системи включає в себе число n – воно є добутком двох простих чисел p та q, що співвідносяться з нерозкладними поліномами. Обирається просте число v.

Секретним ключем являється код B, такий що $(J \otimes B|^v) rem\ n = 1$.

Наприклад, $p = 13$ і $q = 11$ та $v = 23, p \cdot q = n = 11 \cdot 13 = 127$, нехай $J = 19$, тоді $B = 6$.

Процедура ідентифікації віддаленого абонента передбачає наступні дії:

1. Абонент формує випадкове число r, таке, що $1 < r < n - 1$ обчислює значення $T = r|^v\ rem\ n$, та відсилає T в систему.

Нехай $r = 84$, тоді $T = 84|^{23}\ rem\ 127 = 50$.

2. Система генерує випадкове d, яке має знаходитися в діапазоні $0 < d < n - 1$, наприклад, $d = 69$. Це значення також пересилається абоненту.

3. Абонент обчислює $D = r \otimes B|^d\ rem\ n$ та відправляє обчислений код в систему. $D = 84 \otimes 6|^{69}\ rem\ 127 = 51$.

4. В системі вираховується значення

$$T' = D|^v \otimes J|^d rem\ n,$$

якщо $T = T'$, то результат ідентифікації рахується позитивним.

Для приведеного прикладу:

$$T' = 51|^{23} \otimes 19|^{69}\ rem\ 127 = 50.$$

Таким чином, показано, що схеми ідентифікації Шнорра та Гіллоу-Квіскватера працюють при їх реалізації в алгебрі полів Галуа.

Оцінка ефективності запропонованих модифікацій

Для швидкого експоненціювання на полях Галуа може використовуватись наступна властивість поліноміального квадрату $A|^2 = A \otimes A$: його парні двійкові розряди дорівнюють нулю, а непарні – розрядам числа A.

Тобто, якщо

$$A = a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots + a_{n-1} \cdot 2^{(n-1)},$$

де $a_0,..,a_{n-1} \in \{0,1\}$, то

$$A|^2 = a_0 + a_1 \cdot 2^2 + a_2 \cdot 2^4 + \cdots + a_{n-1} \cdot 2^{2\cdot(n-1)}.$$

Таким чином, операція поліноміального піднесення в квадрат зводиться до перестановки розрядів вхідного числа A. Це говорить про те, що в процесі експоненціювання операції піднесення до квадрату можуть не виконуватися , їх результати будуть враховані при множенні на число A. Це дозволяє відразу ж зменшити кількість операцій множення в 3 рази.

Саме множення на постійне число A з редукцією доцільно виконувати з використанням таблиць попередніх обчислень, в яких зберігаються значення

$$A \cdot 2^{\,2} rem\ m, A \cdot 2^{\,4} rem\ m,$$
$$A \cdot 2^{\,6} rem\ m, A \cdot 2^{\,8} rem\ m, \ldots$$

Тоді кожна операція множення на A потребує ,в середньому, $n/2$ звернень до таблиці та операцій логічного додавання. Якщо вважати, що нулі та одиниці в коді експоненти рівноймовірні, то середнє число множень також дорівнює $n/2$, а час Te експоненціювання на полях Галуа, використовуючи вище описаний метод, визначається як:

$$T_e = 0{,}25 \cdot n^2 \cdot s \cdot t_{XT}, \qquad (2)$$

де t_{XT} - час виконання команди XOR, при умові, що один з операндів зчитується з пам'яті (таблиць). Згідно до даних [6] для сучасних процесорів час виконання $t_{XT} \approx \tau$, так, що формула (2) може бути приведена до наступного вигляду:

$$T_e \approx 0{,}25 \cdot n^2 \cdot s \cdot \tau. \qquad (3)$$

В ході порівняння виразів (3) та (1) можна помітити, що значення коефіцієнта прискорення $\beta = \frac{T_M}{Te}$ при переході від модулярного експоненціювання до експоненціювання на полях Галуа визначається виразом :

$$\beta = \frac{T_M}{T_e} \approx \frac{34 \cdot n \cdot s^2}{0{,}25 \cdot n^2 \cdot s} = \frac{136}{w}\ . \qquad (4)$$

З формули (4) слідує, що для 32-розрядного процесора ($w = 32$), коефіцієнт $\beta = 4.25$, а для 8- розрядного контроллера ($w = 8$) $\beta = 17$. Практично це означає, що запропоновані модифікації схем ідентифікації особливо ефективні для малорозрядних вбудованих контролерів, які зараз представляють собою більше половини термінальних пристроїв комп'ютерних систем.

При апаратній реалізації запропонованих модифікацій схем "строгої" ідентифікації досягається суттєво більший виграш у швидкодії в порівнянні з базовими варіантами.

Це зумовлено використанням суматорів без переносу, можливостями паралельної обробки декількох розрядів експоненти. Крім того, досягається значне спрощення схеми.

Висновки

Запропонований та конкретизований для найбільш відомих, основаних на криптографічно строгій концепції "нульового розголошення", схем ідентифікації абонентів підхід підвищення продуктивності програмної та апаратної ідентифікації, що заключається в використанні замість мультиплікативних операцій модулярної арифметики операції поліноміального множення на полях Галуа. Модифіковані методики генерації ключів та процедури ідентифікації на основі принципів "нульового розголошення". Запропоновані ефективні алгоритми програмної реалізації модифікованих схем ідентифікації.

Проведений аналіз показав, що практичне застосування запропонованого підходу забезпечить суттєве (на порядок) збільшення продуктивності ідентифікації при програмній реалізації для систем, термінальними пристроями абонентів яких являються малопотужні портативні контролери з обмеженою споживаною потужністю. Показано, що при апаратній реалізації, запропонований підхід забезпечує значно більше (2-3 порядка) прискорення процесу строгої ідентифікації.

Запропонований підхід і розроблені схеми ідентифікації можуть бути ефективно використані для надійної та швидкої ідентифікації абонентів розподілених систем збору інформації та управління.

Список літератури

1. Bardis N., Doukas N. and Markovskyi O., Fast subscriber identification based on the zero knowledge principle for multimedia content distribution // International Journal of Multimedia Intelligence and Security.- 2010 - Vol.1.- № 4. - P. 363 - 377.

2. Feige U., Fiat A., Shamir. Zero Knowledge Profs of Identity // Journal of Cryptography.- 1988.- v.1- № 2.- P.77-94.

3. Guillou L.C., Quisquater J.-J. A Paradoxical Identity-Based Signature Schemes Resulting from Zero Knowledge // Advances of Cryptology -Crypto-88. Proceeding.- Springer-Verlag.-1990.- P. 216-231.

4. Schnorr C.P. Efficient Signature Generation for Smart Cards // Journal of Cryptology, Vol. 4, No.3.- 1991.- pp.161-174.

6. Montgomery P.L. Modular multiplication without trial division. // Mathematics of Computation, Vol. 44, 1985, pp. 519-521.

7. Брэй Б. Микропроцессоры Intel. Архитектура, программирование и интерфейсы. - СПб.: Изд-во "БХВ-Петрербург".- 2005.- 1328 С.

8. Николайчук Я.М. Коди поля Галуа:теорія і застосування.-Тернопіль:Тов "Терно граф".-2012.- 576 с.

Надійшла до редколегії 1.10.2012

Рецензент: д-р техн. наук. проф. В.Б. Дудикевич, Національний університет «Львівська Політехніка», Львів.

ОДИН ПОДХОД К УСКОРЕНИЮ СТРОГОЙ ИДЕНТИФИКАЦИИ ОТДАЛЕННЫХ АБОНЕНТОВ

А.П. Марковский, И.В. Ткач, Д.Г. Иванов

В статье предлагается подход к ускорению основанной на криптографической строгой концепции "нулевого разглашения" идентификации отдаленных абонентов. Предложенный подход основан на использовании более простои, с точки зрения вычислительной реализации, арифметике конечных полей вместо модулярной арифметики. Теоретически обоснованно и разработаны модификации классических схем строгой идентификации абонентов с использованием предложенного подхода. Работа модифицированных схем идентификации иллюстрируется численными примерами. Теоретическое и экспериментальное исследование разработанных схем доказывает, что предложенный подход позволяет на порядок ускорить программную реализацию идентификации, основанной на криптографической строгой концепции "нулевого разглашения" и на 2-3 порядка – аппаратную.

***Ключевые слова**: строгая идентификация абонентов, концепция нулевого разглашения, арифметика конечных полей, быстрое экспонирование на конечных полях.*

ONE GOING NEAR ACCELERATION OF STRICT AUTHENTICATION OF REMOTE SUBSCRIBERS

A.P. Markovskiy, I.V. Tkach, D.G. Ivanov

In the article offered approach to the acceleration based on cryptographic strict conception of a "zero disclosure" of authentication of remote subscribers. Offered approach based on the use more outages, from point of calculable realization, to arithmetic of the eventual fields in place of modular arithmetic. In theory grounded and modifications of classic charts of strict authentication of subscribers are developed with the use of offered approach. Work of the modified charts of authentication is illustrated numeral examples. Theoretical and experimental research of the developed charts proves that offered approach allows on an order to accelerate programmatic realization of authentication, based on cryptographic strict conception of a "zero disclosure" and on 2-3 orders – vehicle.

***Keywords**: strict authentication of subscribers, conception of a zero disclosure, arithmetic of the eventual fields, rapid exhibiting on the eventual fields.*