УДК 681.3.07

О.А. ШЕВЧУК, І.Д. ГОРБЕНКО

Харківський національний університет радіоелектроніки, Україна

МЕТОД ПРИСКОРЕННЯ СКАЛЯРНОГО МНОЖЕННЯ ДЛЯ КРИПТОГРАФІЧНИХ ДОДАТКІВ

Запропоновано та досліджено метод прискорення обчислення електронного цифрового підпису. Наведено математичну модель методу, необхідні та достатні умови використання методу до існуючих алгоритмів скалярного множення. Досліджено умови ефективності методу, згідно до критеріїв, що запропоновано. Визначено шляхи забезпечення умов ефективності. Наведено приклад застосування до існуючої схеми ЕЦП. Досліджено безпечність схеми ЕЦП після використання методу. Показані недоліки методу, проаналізовано безпечність використання методу. Показано, що за рахунок використання методу можливе отримання прискорення до 25%, з зауваженнями щодо безпечності використання.

Ключові слова: *ЕЦП, скалярне множення, оптимізація обчислень.*

Вступ

У світі набувають практичного використання алгоритми та засоби ЕЦП.

В деяких випадках, при використанні апаратних засобів криптографічного захисту інформації експорт ключових даних ЕЦП заборонено. До таких даних відносяться ключі підтвердження довіреного модуля платформи тощо [3].

У випадку принципової заборони експорту ключових даних, масштабування рішення апаратних засобів криптографічного захисту інформації неможливе.

В статті пропонується метод прискорення операції формування ЕЦП за рахунок зниження стійкості схеми до атаки грубої сили. Розглядається композиція методу з такими методами як COMB та right to left multiplication [2]. Отримана схема дозволяє збільшити швидкодію до 25%. Використання метода може бути доцільним у разі необхідності отримання таких часових характеристик апаратних засобів криптографічного захисту інформації, що неможливо набути існуючими методами.

1. Визначення методу

Метод ґрунтується на збереженні проміжних результатів під час скалярного множення. Метою застосування методу є зменшення часу, необхідного для обчислення скалярного множення, що виконується за допомогою існуючих алгоритмів скалярного множення.

Визначимо функцію

$$\forall X \in GF(q) : \#X = \lfloor \log_2 q \rfloor + 1 .$$

Визначимо пару змінних $k, k' \in GF(q)$, що отримано за допомогою деякої випадкової функції $k \leftarrow \Gamma()$.

Метод може бути застосовано до деякого алгоритму скалярного множення лише за наступних умов.

Якщо $G \in E(GF(q))$, де $E(GF(q))$ -- еліптична крива визначена над $GF(q)$, тоді сумісний алгоритм скалярного множення має бути визначений композицією

$$kG = (f^w_{\#k/w} \circ f^w_{\#k/w-1} \circ \ldots \circ f^w_1)(k, G), \qquad (1)$$

що обчислює результат за $\#k / w$ використань деякої функції

$$f^w_i(k, G) \qquad (2)$$

яка оброблює w бітів з k та вертає деякий проміжний результат, або результат множення. Необхідно відзначити, що окрім обов'язкових параметрів k, G можливе використання додаткових параметрів.

Для (2) має існувати

$$\varphi^w_i(k), \qquad (3)$$

що вертає набір бітів $\{k_\alpha, k_\beta, \ldots\} \in k$ таких, що $\alpha, \beta, \ldots \in [0, \#k]$.

Результат функції (3) має бути необхідним та достатнім для обчислення (2), для неї також має бути справедливе $\forall i \in [1, \#k / w] : \#\varphi^w_i(k) = w$.

Функції (2) та (3) мають бути детермінованими.

Додатково визначимо

$$\Phi^w(i,k) = \varphi^w_i(k) \| \varphi^w_{i-1}(k) \| \ldots \| \varphi^w_1(k),$$

таку що $\#\Phi^w(i,k) = w*i$.

Нескладно побачити, що для пари k, k', та $\xi \le \#k / w$, де $\forall i \in [1,\xi]: \varphi_i^w(k) = \varphi_i^w(k')$, справедливі наступні твердження:

- $f_\xi^w(k,G)=f_\xi^w(k',G)$;
- якщо $\#k/w-\xi>0$, тоді $kG \ne k'G$;
- якщо $\nu = \#k / w - \xi$, тоді відстань Геммінга $d(k,k') \le \nu * w$.

Методом пропонується зберігати $f_\xi^w(k,G)$, та використовувати його при обчисленні $f_{\#k'}^w(k',G)$.

Визначимо показник ефективності методу як

$$\Delta = P_m \frac{T-M}{T}, \qquad (4)$$

де T – кількість виконань функції $f_i^w(k,G)$ для отримання пари точок $kG, k'G$ з $k,k' \in GF(q)$, $\xi \in [0,\#k/w]$, $\forall i \in [1,\xi]: \varphi_i^w(k) = \varphi_i^{'w}(k)$, $G \in E(GF(q))$ існуючими методами, M – запропонованим методом, та P_m – ймовірність можливості застосування методу.

Далі будемо вважати, що метод є ефективним, коли $\Delta > 0{,}15$, та мінімальна складність атаки повного розкриття не зменшується після впровадження методу.

2. Аналіз ефективності методу

Ґрунтуючись на визначених твердженнях, обчислимо необхідну кількість обчислень для виконання пари скалярних множень.

У традиційний спосіб, для обчислення пари точок з необхідно виконання $T=2\#k/w$ функцій $f_i^w(k,G)$. Не складно побачити, що у разі збереження проміжного результату, можливо отримати пару результатів $kG, k'G$ за $M = (2\#k / w - \xi)$ виконань функцій $f_i^w(k,G)$.

Ймовірність використання методу P_m для двох випадкових k, k', може бути оцінена як

$$P(\xi,k,w)=\frac{1}{2^{\xi * w}}. \qquad (5)$$

Тоді, для визначеного випадку

$$\Delta_\xi = P_m \frac{T-M}{T} =$$

$$= P(\xi,k,w)\frac{2\#k / w - (2\#k / w - \xi)}{2\#k / w} =$$

$$= \left(\frac{1}{2^{\xi * w}}\right)\left(\frac{\xi}{2\#k / w}\right) = \frac{w\xi}{\#k 2^{\xi * w+1}}.$$

Знайдемо максимум отриманої функції.

Якщо $\Delta'_\xi = \frac{w2^{-w\xi-1}}{k} - \frac{\log(2)w^2\xi 2^{-w\xi-1}}{k}$,

$$\frac{w2^{-w\xi-1}}{k} - \frac{\log(2)w^2\xi 2^{-w\xi-1}}{k} \overset{k>0}{\Leftrightarrow}$$

$$\Leftrightarrow w2^{-w\xi-1} - \log(2)w^2\xi 2^{-w\xi-1} = 0 \Leftrightarrow$$

тоді

$$\Leftrightarrow w2^{-w\xi-1} = \log(2)w^2\xi 2^{-w\xi-1} \overset{w>0}{\Leftrightarrow}$$

$$\Leftrightarrow w = \log(2)w^2\xi \Leftrightarrow$$

$$\Leftrightarrow \xi = \frac{1}{w\log(2)}$$

та мінімальне $w = 1$, тоді максимум $\max \Delta_\xi \approx 0{,}002$, що менший ніж визначений критерій ефективності.

Для того, щоб покращити результат, необхідно значно збільшити $P(\xi,k,w)$. Якщо існують такі умови, для яких $P(\xi,k,w)=const=1$, тоді

$$\Delta_\xi = P_m \frac{T-M}{T} = \frac{2\#k / w - (2\#k / w - \xi)}{2\#k / w} = \frac{\xi}{2\#k / w}, \qquad (6)$$

що монотонно зростає, та набуває $\max \Delta_\xi = 0{,}5$.

Нагадаємо, що у випадку

$$\forall i \in [1,\xi * w]: \varphi_i^w(k) = \varphi_i^w(k') \qquad (7)$$

ймовірність використання методу $P(\xi,k',w) = 1$.

Таким чином, у разі забезпечення дійсності (7) також вирішується задача забезпечення умов.

Пропонується коригувати метод формування множників k, k'. Нагадаємо, що k, k' формуються за допомогою деякої функції $\Gamma()$. Пропонується змінити $\Gamma()$ на композицію $\Gamma'() = (\alpha_\gamma \circ \Gamma)()$, де для деякої функції $\alpha_\gamma(x): \Gamma'() \to k,\ \Gamma'() \to k'$ що забезпечує (7). Параметр γ вказує на кількість попередніх використання функції.

Визначимо таку константу μ^w, для якої дійсне наступне твердження:

$$\begin{cases} \Phi^w(i,\mu_i^w) = \#\{1_0,1_1,\ldots,1_w\}; \\ \forall x \in GF(q): d(\mu_i^w,x) = \#x - \#\Phi^w(i,\mu_i^w). \end{cases}$$

Тобто μ_i^w визначає таку бітову маску, що покриває усі біти використанні при обчисленні $\Phi^w(i,x)$ та тільки їх.

Визначимо функтор $\alpha_\gamma(x)$ такий що

$$\alpha_\gamma(x) := \left| \begin{array}{l} \gamma \equiv 0 \bmod 2 : x; \\ \gamma \equiv 1 \bmod 2 : (A_{\gamma-1} \,\&\, \mu) \,|\, (\neg\mu \,\&\, x), \end{array} \right. \qquad (8)$$

де $A_{\gamma-1}$ -- результат виконання $\alpha_{\gamma-1}$.

Таким чином, для забезпечення ефективності методу необхідно забезпечити додаткові умови до множників.

3. Приклад застосування методу до існуючих алгоритмів скалярного множення

Наступним кроком необхідно модифікувати метод скалярного множення, що використовується. Модифікація можлива, якщо метод скалярного множення можливо визначити у вигляді (1). Наприклад, для методу right-to-left binary method (RLBM) [2] :

$$f_j^1(k,P,Q) := \begin{vmatrix} j = \#k & : & Q; \\ \#k > j > 1 & : & f_{j-1}^1(k, P+P, \left(Q+\varphi_j^1(k)P\right)); \\ j = 1 & : & (P+P, \varphi_j^1(k)P), \end{vmatrix} \quad (9)$$

та для COMB методу з передобчисленнями [2] :

$$f_j^w(k,P,A,B) = \begin{vmatrix} j = \#k/w & : & A; \\ \#k/w > j > 1 & : & f_{\#k/w-j-1}^1(k,P,A+\beta,\beta), \\ & & \beta = B + PR(P, \varphi_{\#k/w-j}^1(k)); \\ j = 1 & : & (P,\beta,\beta), \\ & & \beta = \infty + PR(P, \varphi_{\#k/w}^1(k)); \end{vmatrix} \quad (10)$$

де $PR(P,\varphi_j^w(k))$ – функція що вертає точку з таблиці передобчислень для точки P.

Для обраного методу необхідно визначити $\varphi_i^w(k)$. Наприклад, для RLBM

$$\varphi_i^1(k) = \{k_{i-1}\} \quad (11)$$

а для COMB:

$$\varphi_i^w(k) = \{k_{dw+i}, k_{d(w-1)+i}, \ldots, k_i\}, d = \lfloor \#k/w \rfloor. \quad (12)$$

Тоді необхідно модифікувати алгоритм множення. Наприклад, згідно до (8) до алгоритму (9) необхідно визначити функтор кешування

$$C_\gamma(X) = \begin{cases} \gamma \equiv 0 \bmod 2 : X; \\ \gamma \equiv 1 \bmod 2 : \Theta, \end{cases} \quad (13)$$

де Θ_γ -- результат, що було отримано з C_γ на γ виклику.

$$j = \xi : C_\gamma(f_{j-1}^1(k, P+P, \left(Q+\varphi_j^1(k)P\right))) \quad (14)$$

та до (10) за аналогією.

Таким чином, наведені алгоритми є сумісними з методом.

4. Аналіз стійкості схеми ЕЦП, що використовує метод, до атаки грубої сили

Виконаємо аналіз на прикладі схем ЕЦП з доданком, що ґрунтуються на схемах похідних з DSA [1] та ECNR [4] .

Як було зазначено, для ефективного використання методу необхідно забезпечити $P_m = 1$. Запропонована функція (8) утворює композицію з генератором множників $\Gamma()$. Пропонується використовувати метод у схемах ЕЦП на етапі формування сесійного ключа. Тут і надалі для сесійного ключа підпису використаємо позначення k, так як сесійний ключ передпідпису задовольняє вже наданому визначенню. Тоді, в схемі ЕЦП, де сесійний ключ визначається як $k = PRNG()$ (тобто $\Gamma = PRNG()$), необхідно змінити визначення на $k = (\alpha_\gamma \circ PRNG)() = \Gamma'()$.

Відображення результатів генератору псевдовипадкових послідовностей за допомогою (8) порушує вимоги до сесійного ключа ЕЦП. Дійсно, для усіх класів ЕЦП, що базуються на DLP/ECDLP, щодо сесійних ключів висуваються такі вимоги:

– сесійний ключ k має бути негайно знищено;

– сесійний ключ k не має бути пов'язаним з іншими k, ніякими співвідношеннями.

Легко побачити, що в (8) по-перше частково зберігається попереднє значення k, по-друге формується зв'язок між попереднім та наступним значенням k за одне з трьох формувань.

Проаналізуємо вплив з використання методу на загальну безпечність схем ЕЦП, на прикладі ECNR.

Підпис ECNR обчислюється як

$$\{r = f(M) + \Pi; s = (k - X_a r); \bmod N\},$$

де $\Pi = kG$, $f(M)$ - деяке відображення повідомлення, до поля обчислення підпису, X_a - секретний ключ користувача, а Q_a - відкритий. Стійкість підпису ґрунтується на складності пошуку такого k', що $k'G = kG$, чи деякого $\xi = k_1 - k_2$ для пари підписів $(r_1, s_1).(r_2, s_2)$, для якого

$$\left(\frac{\xi - s_1 + s_2}{r_2 - r_1}\right) G = Q_a \bmod N. \quad (15)$$

Розглянемо існуючі шляхи пошуку $k'G = kG$.

Існує значна кількість шляхів вирішення задачі ECDLP, серед яких найбільш раціональними є алгоритми ρ,λ - Полларда, що мають складність порядку $O(\sqrt{n})$, де n -- порядок базової точки.

– Алгоритм ρ - Полларда. Для виконання алгоритму необхідно порядку

$$\sqrt{\pi n/2} + O(\log n) \quad (16)$$

групових операцій [5].

– Алгоритм λ - Поларда потребує порядку $O\left(3{,}3\sqrt{n}\right)$, або $O\left(2\sqrt{n}\right)$ групових операцій, при дворазовому збільшенні пам'яті та двох процесів виконання[5].

– У разі використання алгоритму λ-Полларда або Van Oorschot, Wiener, необхідно порядку $O(2\sqrt{n}/r+1/\Theta)$ групових операцій, де r – кількість процесорів, Θ - частина позначених точок.

В існуючих версіях алгоритмів ρ,λ-Полларда, та похідних з них, інформація про частковий зв'язок не використовується.

Вирішення задачі $(k_1'G = k_1G, k_2'G = k_2G)$ для випадку, коли

$$\left(k_1 = \alpha_0(PRNG()), k_2 = \alpha_1(PRNG())\right)$$

зводиться до визначення наступної проблеми. Чи можливе створення такого метода факторизації, що на вхід прийме $n, n > 2$ точок $(k_1G, k_2G, \ldots k_nG)$, і $\Phi^w(\xi, k)$, де $\forall k \in (k_1, k_2, \ldots k_n)$, та вирішить задачу пошуку k′G=kG зі складністю меншою, ніж існуючі?

Оцінимо складність кращого випадку вирішення (15). Якщо відоме $\Phi^w(\xi, k)$, тоді для пари $k_2 - k_1$, що сформовано за допомогою (8), вага Хаффмана d=#G-mw. Тоді задачу пошуку можна вирішити за O(d) операцій (15), формуючи ξ за деяким законом $\alpha'()$, що враховуючи позиції відомо однакових бітів у k_2, k_1 встановлює значення цих бітів у 0.

Якщо твердження вірні, тоді метод є безпечним, доки $\left(\#k - \#\Phi^w(\xi, k)\right) > \sqrt{\#k}$, тобто

$$\#k - \#k^{-1} > 2^{\xi * w} \qquad (17)$$

Тоді, для ЕК $GF(q), P = 2^{160}$, $w = 8$ безпечне $\xi < 10$.

За визначених умов стійкість методу відповідає критеріям.

5. Експериментальні дослідження

Для перевірки (4) у разі $P_m = 1$ імплеметовано (8) для Comb методу з передобчисленнями з вікном 8, у GF(p).

На рис. 1 показана отримана залежність використаного часу від обраного ξ.

Обчислимо очікуване (4) для

$$x = 8, w = 8, \#k = 160:$$

$$\Delta = \frac{w\xi}{2\#k} = \frac{8*8}{2*160} = 0,2. \qquad (18)$$

Обчислимо отримане в результаті експерименту (M = 37c , T = 52c , Atom N550, 100000 ітерацій):

$$\Delta = \frac{52 - 37}{52} \approx 0,28. \qquad (19)$$

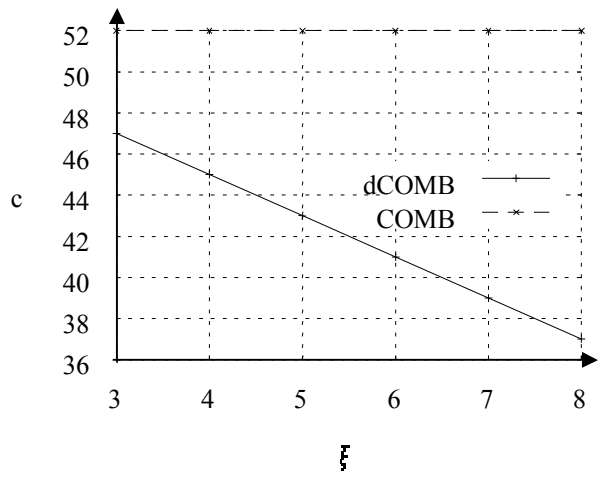

Рис. 1. Залежність використаного часу від обраного ξ

Розбіжності між розрахованим та отриманим результатами пояснюються особливістю реалізації (введено додаткову економію подвоєння точки).

Приклад авторської програмної реалізації розташовано за такою адресою:
https://iso-iec-9796-3.googlecode.com/, гілка decomb.

Висновки

В статті запропоновано метод, що покращує часові характеристики формування цифрового підпису, що виконується у групі точок еліптичних кривих за рахунок зменшення стійкості до атаки грубої сили.

Метод дозволяє отримати прискорення операції формування ЕЦП до 25% за рахунок зниження стійкості схеми ЕЦП до атаки грубої сили у гіршому випадку.

У разі використання методу, криптоаналітик отримує додаткову інформацію про кореляційні властивості вхідних даних. На час аналізу не існувало методу пошуку дискретного логарифму у групі точок еліптичних кривих, що за рахунок додаткової інформації дає можливість вирішити проблему з меншою складністю, ніж алгоритми що відомі на цей час.

Результати оцінки прискорення, що отримані в ході експерименту, не суперечать отриманим теоретично.

Література

1. Digital Signature Standart [Text]. - (DSS): FIPS 186-3.

2. Hankerson, D. Guide to Elliptic Curve Cryptography [Text] / D. Hankerson, A.J. Menezes, S. Vanstone. – Jan., 2004.

3. ISO/IEC 11889-2:2009 Information technology. –Trusted Platform Module – Part 2: Design principles [Text]. – 2009.

4. ISO/IEC 9796-3: Discrete logarithm based mechanisms [Text]. – 2006.

5. Lower bounds for discrete logarithms and related problems [Text] // Advances in Cryptology. EUROCRYPT'97. – 1997.

Поступила в редакцию 2.03.2012

Рецензент: д-р техн. наук, проф. А.В. Скатков, Севастопольський національний технічний університет, Севастополь, Україна.

МЕТОД УСКОРЕНИЯ СКАЛЯРНОГО УМНОЖЕНИЯ ДЛЯ КРИПТОГРАФИЧЕСКИХ ПРИЛОЖЕНИЙ

А.А. Шевчук, И.Д. Горбенко

Предложен и исследован метод ускорения вычисления электронной цифровой подписи. Приведена математическая модель метода, необходимые и достаточные условия применения метода к существующим алгоритмам скалярного умножения. Исследованы условия эффективности метода, относительно предложенного критерия. Определены способы удовлетворения условий эффективности. Приведены примеры применения метода к существующей схеме ЭЦП. Исследовано влияние метода на безопасность схемы ЭЦП после использования метода. Показаны недостатки метода. Показано, что с использованием метода можно увеличить скорость формирования ЭЦП до 25%, с некоторыми замечаниями к безопасности.

Ключевые слова: ЭЦП, скалярное умножение, оптимизация вычислений.

METHOD OF ACCELERATION OF SCALAR MULTIPLICATION FOR CRYPTOGRAPHIC SCHEMES

A.A. Shevchuk, I.D. Gorbenko

The calculation acceleration method of the electronic digital signature is offered and investigated. The mathematical model of the method, necessary and sufficient conditions of application of a method is resulted in existing algorithms of scalar multiplication. Conditions of efficiency of a method, concerning the offered criterion are investigated. Ways of satisfaction of conditions of efficiency are defined. Examples of application of a method are led to existing scheme DSS. Influence of a method on safety of scheme DSS after method use is investigated. Method lacks are shown. It is shown that with method use it is possible to increase speed of formation DSS to 25 %, with some remarks to safety.

Key words: DSS, scalar multiplication, optimization of calculations.

Шевчук Олексій Анатолійович – аспірант каф. БІТ Харківського національного університету радіоелектроніки. E-mail: alxchk@gmail.com.

Горбенко Іван Дмитрович – д-р техн. наук, проф., зав. каф. БІТ Харківського національного університету радіоелектроніки.