Модулна редукция за криптографски алгоритми без предварителни изчисления

Пламен Стоянов, Валентин Димов

Modular reduction for cryptographyc algorithms without pre-calculation: *One of the most important features of the communications systems ourdays is the data transmission security. One major factor that determines the performance of the cryptographic algorithms is a class of modular operations - A^E mod M. There are some algorithms invented in order to decrease the computation time of this division, from which the most popular are the Montgomery u Barrett ones. This work focuses on another approach for performance improvement, that does not need pre-calculation in order to implement modular reduction and multi-digit division. The new approach consists of finding the whole part Q and the remainder R with modulis (M+p). Using Q(M+p)+R we can calculate the remainder of interest.*

Key words: *modulus operation, reduction, assymetrycal algorithms.*

ВЪВЕДЕНИЕ

Една от най-важните характеристики на комуникационните системи е сигурността при обмен на информация. Потребителите изискват защита на информацията от неоторизиран достъп и преправяне. Основно средство за постигане на целта е използването на криптографията. Чрез криптографски алгоритми, входните данни (открит текст) се преобразуват в шифротекст използвайки определени функционални зависимости. Процесът на преобразуване на открития текст се обозначава като шифриране (криптиране), а обратното преобразуване като дешифриране (декриптиране). В процеса на преобразуване на данните се използва ключ, който може да бъде еднакъв при шифриране и дешифриране. В този случай криптографските алгоритми се наричат симетрични [6]. Най-често използвани са блоковите шифри – Triple DES, IDEA, RC5 и др. Повечето от тях се основават на идеята на Horst Feistel за разделяне на входния блок на две части L и R, и извършване на итеративни преобразувания на тези части. Криптографските алгоритми се наричат асиметрични (алгоритми с публичен ключ), когато ключовете за шифриране и дешифриране са различни. Най-популярни са RSA, Diffe-Helman, ECC, като RSA е с преобладаващо значение. Основна операция при тези алгоритми е модулната редукция $A^E \bmod M$ (A<M) , където A е основата, E е степента и M е модулът. При наличието на вградени хардуерни умножители в използваните микроконтролери, времето за криптиране и декриптиране основно се определя от операциите за извършване на многоразрядно целочислено деление. При RSA първоначално се препоръчва 200 цифров ключ [7], но поради нарастналите изчислителни възможности понастоящем се използва 2048 битов ключ . Най известните алгоритми за съкращаване времето за изпълнение са алгоритмите на Montgomery и Barrett. Идеята е промяна на модула с кратен на машинната дума или по-голям, при което операциите се свеждат до преместване и ротация. Недостатък е , че се извършват предварителни изчисления използващи целочислено деление на зададения модул. Ефективни са при криптиране и декриптиране на по-голям обем информация, при което се изпълняват многократни операции при еднакъв модул. При по-малки по обем съобщения (примерно обмен на сесийни ключове за симетрични алгоритми), времето за изпълнение е сравнимо с класическия алгоритъм.

В разработката се предлага алгоритъм за модулна редукция без използване на предварителни изчисления и многоразрядно деление. Намира се цялата част Q и остатъка R при модул (M+p). Чрез Q(M+p)+R се намира търсения остатък. Изчисленията се свеждат до умножение и преместване, тъй като $M+p = 2^{n+1}$, където n е разрядността на зададения модул. В някои случаи се получава резултат по-

голям от M ,при което се налага корекция но не по-вече от един път (при Barrett корекцията е не по-вече от 2).

АЛГОРИТМИ ЗА МОДУЛНА РЕДУКЦИЯ

За намаляване времето за изпълнение на модулните операции, най-често се използват алгоритъм на Barrett и алгоритъм на Montgomery. Променя се модула с кратен на машинната дума. Paul Barrett [1] предлага за намиране на X=A mod M, вместо целочисчено деление да се използва умножение, което изисква по-малко време за изпълнение. Изразът X=A – M*$\lfloor A/M \rfloor$, се променя на X=A-M*(A*R). Тъй като R е по-малко от 1, за представянето му като целочислено, се извършва предварителната операция R=$\lfloor b^{2n}/M \rfloor$, където b е основата на модула и n е неговата разрядност. Изчислява се цялата част $\bar{Y}$ = $\lfloor A/b^{n-1} \rfloor$ * $\lfloor b^{2n}/M \rfloor$ / b^{n+1} , след което се намира остатъка. Тъй като остатъка от целочислените деления $\lfloor A/b^{n-1} \rfloor$ и $\lfloor b^{2n}/M \rfloor$ не участва в изчисленията, в някои случаи (според Barrett не по-вече от 10%) се получава $\bar{X} \geq$ M и се налага корекция на резултата. Направени са множество предложения за повишаване ефективността на алгоритъма[3,8].

P. Montgomery предлага оригинален алгоритъм [5] за намиране на TmodN . Избира се основа R=b^n като R>N и gcd(R,N)=1. Необходимо е N` и $R^{-1}$ да удовлетворяват условието R*$R^{-1}$ - N*N` = 1. Чрез функцията REDC(T) се намира t = T R^{-1} mod N.

```
Function REDC(T)
m ← (T mod R)N` mod R
t ← (T+mN)/R
if t ≥ N then return t-N else return t
```

За намиране на действителното T mod N, отново се изпълнява функцията, при REDC(t mod N)(R^2 mod N). Cetin Koc [4] анализира 5 варианта основани на този алгоритъм. Bosselaers [2] сравнява времената за модулна редукция при различна дължина на модула (до 1024 бита) на три алгоритъма – класически, Montgomery и Barrrett.

Разгледаните алгоритми се използват при обработка на информация с голям обем, тъй като се работи с различна основа A и еднакъв модул M. Поради наличието на предварителни изчисления (R^{-1} и N` при Montgomery и $\lfloor b^{2n}/M \rfloor$ при Barrett) при криптиране на кратки съощения, класическият алгоритъм с традиционно деление е по-бърз. При системата PGP [9], се използва комбинация от асиметричният алгоритъм RSA и симетричния IDEA.

АЛГОРИТЪМ БЕЗ ПРЕДВАРИТЕЛНИ ИЗЧИСЛЕНИЯ

За намиране на R = A mod M, може да се представи

$$A = Q_1 * M + R_1 \qquad (1)$$

където Q_1 е цялата част и R_1 = R е търсеният остатък. Използваната основа е b, M < b^n и условие A < b^{2n}. Чрез преместване без използване на традиционно деление, лесно се намира R_2 = A mod b^n. Тъй като M < b^n може да се изчисли P = b^n - M. Представя се:

$$A = Q_2 * (M + P) + R_2 \qquad (2)$$

От (1) и (2) следва: $R_1 = A - Q_1 * M = Q_2 * M + Q_2 * P + R_2 - Q_1 * M$

$$R_1 = (Q_2 - Q_1) * M + Q_2 * P + R_2$$

Тъй като (Q_2 - Q_1) * M mod M = 0 и R_1 < M, то

$$R_1 \equiv (Q_2 * P + R_2) \bmod M \quad (3)$$

При получаване на резултат по-голям от M, е необходимо (3) да се изчисли повторно. Обобщено може да се запише:

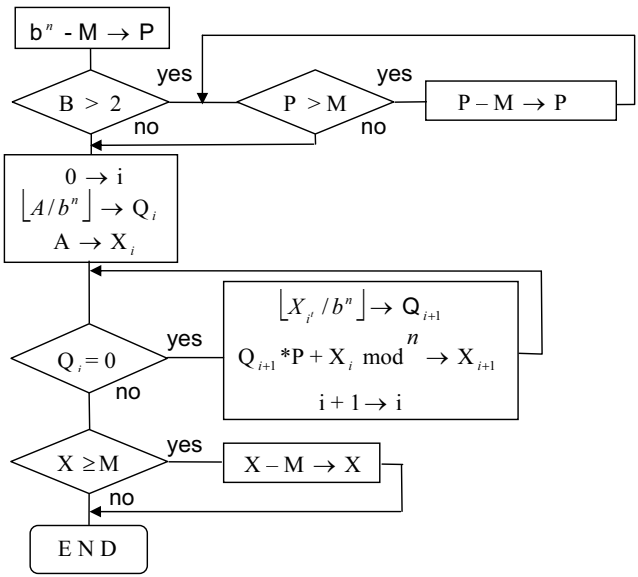
$$R_1 \equiv (Q_i * P + R_i) \bmod M \quad (4)$$

Q_i е винаги по-малко от M поне с един разряд в основа b. При използване на сестема различна от b=2, е възможно да се получи P > M и $(Q_i * P + R_i) > A$. В тези случаи е необходимо преди умножението $Q_i * P$, да се проверява стойността на P. Ако P > M , се извършва $P_j = P_{j-1} - M$ докато се получи $P_j < M$. Тъй като $Q_i < M$ и P<M, то за намиране на X са необходими краен брой изчисления (4). Колкото е по-малка стойността на P, толкова по-висока е изчислителната ефективност. Предимство е, че умноженията не надхвърлят двойна точност и разредността на множимото намалява след всяка стъпка. За намиране R = A mod M се предлага следният алгоритъм в операторен вид и като блок-схема :

Input : $A = (a_{2n-1} \ldots a_1\ a_0)_b$, $M = (m_{n-1} \ldots m_1\ m_0)_b$, $A < M^2$

Output: $X = (x_{n-1} \ldots x_1\ x_0)_b = A \bmod M$

1. $i \leftarrow 0$, $P = b^n - M$
   if b >2 then while P > M do P = P – M
   $Q_0 \leftarrow \lfloor A/b^n \rfloor$, $X \leftarrow A$
2. while $Q_i > 0$ do :
   2.1 $Q_{i+1} \leftarrow \lfloor X_{i'}/b^n \rfloor$
   2.2 $X_{i+1} \leftarrow Q_{i+1} * P + X_i \bmod b^n \rightarrow$
   2.3 $i \leftarrow i + 1$
3. if $X \geq M$ then $X \leftarrow X - M$



Пример: X = 219382 mod 487, b=10, n=3

1. $P = 10^3 - 487 = 513$, $P = 513 - 487 = 26$
2. 219*26 + 382 = 6076
   6*26 + 76 = 232
3. резултат X=232, X < M корекция не се налага

ЗАКЛЮЧЕНИЕ

Криптирането и декриптирането чрез асиметрични алгоритми е по-бавно в сравнение със симетричните. При по-малък обем на информацията, традиционните алгоритми (на Barrett и Montgomery) са по-бавни поради извършване на необходими предварителни изчисления. Предложеният алгоритъм за модулна редукция е ефективен при предаване на кратки съобщения. Той е по-бърз от класическият алгоритъм, тъй като целочисленото деление се замества с преместване и ротация. Може да се използва при обмен на сесийни ключове за симетрични алгоритми и разпознаване. При използване на алгоритъма за система различна от двоичната, се предлага предварителна проверка. Ако P > M , се извършва корекцията P = P – M. В този случай се намаляват циклите в стъпка 2 от алгоритъма, което води до повишаване на общото бързодействие. В двоична система, проверката P > M може да се използва при допълване на n до кратно на 8 бита, чрез което се премахват ротациите в стъпка 2.1 за намиране на Q_{i+1}.

ЛИТЕРАТУРА

[1] Barrett,P., Implementing the Rivest Shamir Adleman public-key encrypton algorithm on a standart digital signal processor. Advances in Cryptology – CRYPTO'86, pp. 311-323, 1987

[2] Bosselaers,A., R.Govaerts, J.Vandewalle, Comparision of three modular reductions. Advances in Cryptology – Crypto'93 (LNCS 773), Springer-Verlag,pp.175-186, 1994.

[3] Hasenplaugh,W., G.Gaubatz, V.Gopal. Fast Modular Reduction. IEEE Symposium on Computer Arithmetic, Montpellier, pp. 225-229, 2007.

[4] Koc,C., R.Govaerts, B.Kaliski. Analyzing and comparing Montgomery multiplication algorithms. IEEE Micro, vol.16, pp.26-33, 1996

[5] Montgomery,P. Modular multiplication without trial division. Matematics of Computation, vol.44, pp.519-521, 1985.

[6] Rankl,W., W.Effing. Smart card handbook. Carl Hanser Verlag, Munich, 2002.

[7] Rivest,R., A.Shamir, L.Adleman. A method for obtaining for digital signatures and public-key cryptosystems. CACM, vol.21, pp.120-126, 1978'

[8] Stoianov,P., R.Dimova. Reduction of correction in Barrett's algorithm. ICEST'08, Serbia, vol.1, pp.500-503, 2008

[9] Антонов,П., С.Малчев. Криптография в компютърните комуникации. Варна, 2000.

За контакти:

Гл. ас. Пламен Стоянов, Катедра "Съобщителна техника", Технически университет – Варна, тел. 052 383 517, e-mail: pl63@abv.bg

Гл. ас. Валентин Димов, катедра "Електронна техника и микроелектроника", Технически университет – Варна

Докладът е рецензиран.