Metoda Lenstry-Shora faktoryzacji dużych liczb całkowitych

Tomasz Stroiński

23.06.2014

Po co faktoryzować tak duże liczby?

System RSA

Działanie systemu RSA

· Każdy użytkownik wybiera duże liczby pierwsze p, q.

· Użytkownik wykonuje proste mnożenie $n = pq$

· Znając rozkład n na czynniki użytkownik wylicza $\varphi(n) = (p-1)(q-1) = n+1-p-q$

· Użytkownik wybiera losowo liczbę całkowitą e z przedziału $(1, \varphi(n))$, względnie pierwszą z $\varphi(n)$

· Użytkownik wylicza $d := e^{-1} \mod \varphi(n)$

· Klucz szyfrujący (n, e) publikuje się, natomiast klucz deszyfrujący (n, d) pozostawia w tajemnicy.

· Wiadomość M szyfrujemy do postaci szyfrogramu $C := M^e \pmod n$

· Odzyskanie wiadomości M z szyfrogramu C polega na policzeniu $M = C^d \pmod n$

Uwagi:

· Losowość wyboru liczby e jest osobnym zagadnieniem kryptograficznym

· Podobnie jak wybór przekształcenia wiadomości stworzonej na podstawie alfabetu na system liczbowy

· Bezpieczeństwo tego systemu opiera się na trudności w faktoryzacji liczby n

· Liczby n i e podawane są do publicznej wiadomości, więc obliczenie d i odszyfrowanie wiadomości przy znajomości faktoryzacji liczby n nie jest problemem.

Bezpieczeństwo RSA

· RSA Security ogłasza RSA Factoring Challenge (1991) i publikuje listę liczb RSA

· Kolejne osiągnięcia (sfaktoryzowane liczby) wpływają na długość używanych kluczy

· RSA Security zamyka konkurs (2007) uznając, że istnieją lepsze metody sprawdzania bezpieczeństwa algo-

rytmów, których podstawą jest trudność faktoryzacji dużych liczb pierwszych.

· W 2009 roku następuje faktoryzacja liczby RSA-768 za pomocą algorytmu opartego na metodzie sita ciała liczbowego

· Jest to największa liczba RSA sfaktoryzowana do tej pory (publikacja - eprint.iacr.org/2010/006.pdf)

Jak wykonać taką faktoryzację?

Idea

· Szukamy $x \not\equiv \pm y \pmod{n}$, aby $x^2 \equiv y^2 \pmod{n}$

· Wtedy $\text{nwd}(x - y, n)$ jest nietrywialnym dzielnikiem n

Metoda ułamków łańcuchowych

· Wybieramy redukty $\frac{x_i}{y_i}$ z ułamka łańcuchowego $\sqrt{n}$

· Tworzymy $Q_i = {x_i}^2 - n{y_i}^2$, wtedy $|Q_i| < 2\sqrt{n}$

· Wybieramy gładkie Q_i

· Wybieramy zbiór indeksów I tak, aby $\Pi_{i \in I}\ Q_i$ był kwadratem pewnej liczby

· Niech $y^2 = \Pi_{i \in I}\ Q_i$

· Wtedy $(\Pi_{i \in I}\ x_i)^2 \equiv y^2 \pmod{n}$ jest poszukiwaną kongruencją

Metoda sita kwadratowego

· Wybieramy wielomian $Q(X) = X^2 - n$

· Wybieramy x spełniające dla pewnego $M > 0$ warunek $|x - \sqrt{n}| < M$

· Mamy wtedy, że $|Q(x)|$ jest niewiele większa od $2M\sqrt{n}$

· Wartości $Q(x)$ mogą być większe niż Q_i dla metody ułamków łańcuchowych, lecz gładkość można sprawdzać korzystając z sita.

· Dla gładkich $Q(x)$ konstruujemy taki podzbiór argumentów S, aby produkt $\Pi_{x \in S} Q(x)$ był kwadratem

· Oznaczmy $y^2 = \Pi_{x \in S} Q(x)$

· Wtedy $(\Pi_{x \in S} x)^2 \equiv y^2 \pmod{n}$ jest poszukiwaną kongruencją

Wydobycie rozkładu n

· Konstruujemy przekształcenie $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

· dla metody ułamka łańcuchowego $(x_i^2, x_i^2 - ny_i^2) \xrightarrow{\phi} (x_i^2, x_i^2)$

· dla metody sita kwadratowego $(x^2, x^2 - n) \xrightarrow{\phi} (x^2, x^2)$

· Przy odrobinie szczęścia $\phi(x, y) \notin D := \{(x, \pm x) : x \in \mathbb{Z}/n\mathbb{Z}\}$

Metoda sita ciała liczbowego

· Powyższe metody potrzebują wielu wartości $Q(x)$, bądź Q_i aby uzyskać odpowiednią liczbę gładkich wartości

· Metoda sita ciała liczbowego potrzebuje do tego znacznie mniej wartości

Idea

· Tworzymy analogiczne przekształcenie $\phi : \mathbb{Z} \times \mathbb{Z}[\alpha] \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

· Działamy teraz na $(x^2, \beta^2) \in \mathbb{Z} \times \mathbb{Z}[\alpha]$

· Otrzymujemy kongruencję $x^2 \equiv \phi(\beta)^2 \pmod{n}$

Rozwinięcie metody

· Wykorzystamy normę $N : \mathbb{Q}(\alpha) \to \mathbb{Q}$, spełniającą dla $x \in \mathbb{Z}[\alpha]$ warunek $|N(x)| = \#(\mathbb{Z}[\alpha]/x\mathbb{Z}[\alpha])$

· Natomiast dla elementu $x = a - b\alpha \in \mathbb{Q}(\alpha)$, przy $f(x) = \sum_{i=0}^{d} c_i x^i$ $N(a - b\alpha) = b^d f(\frac{a}{b}) = \sum_{i=0}^{d} c_i a^i b^{d-i}$

· Tworzymy homomorfizm $\phi : \mathbb{Z}[\alpha] \to \mathbb{Z}/n\mathbb{Z}$, aby $\phi(1) = 1 \pmod{n}$ oraz $\phi(\alpha) = m \pmod{n}$, gdzie m jest pierwiastkiem wielomianu $(f \bmod n)$

· Jeżeli wybierzemy f i będziemy poszukiwać odpowiedniego m, będzie to zdecydowanie trudniejsze niż obranie m

· Wybieramy $m = \lfloor n^{\frac{1}{d}} \rfloor$ i zapisujemy n w bazie $(1, m, ..., m^d)$, czyli $n = \sum_{i=0}^{d} c_i m^i$

· Wtedy $f(X) = \sum_{i=0}^{d} c_i X^i$ jest odpowiednim wielomianem, który spełnia $f(m) = n$, co daje $f(m) \equiv 0 \pmod{n}$

· Określamy $\phi : \mathbb{Z} \times \mathbb{Z}[\alpha] \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ zachowujące własności jak wyżej

· Wtedy $\phi(a - bm, a - b\alpha)$ jest postaci (x, x)

· Poszukujemy teraz zbioru S zawierającego takie pary (a, b), aby $\text{nwd}(a, b) = 1$ oraz by

(*) $\Pi_{(a,b)\in S}(a-bm)$ był kwadratem w $\mathbb{Z}$ oraz

(**) $\Pi_{(a,b)\in S}(a-b\alpha)$ był kwadratem w $\mathbb{Z}[\alpha]$

· Niech zatem $\Pi_{(a,b)\in S}(a-bm)=y^2$, a $\Pi_{(a,b)\in S}(a-b\alpha)=\beta^2$ oraz $x=\phi(\beta)$

· Wtedy $x^2=\phi(\beta)\phi(\beta)=\phi(\beta^2)=\phi(\Pi_{(a,b)\in S}(a-b\alpha))=\Pi_{(a,b)\in S}\phi(a-b\alpha)\equiv\Pi_{(a,b)\in S}\phi(a-bm)=y^2$.

· Stąd mamy kongruencję $x^2\equiv y^2 \pmod{n}$

· Chcemy teraz tak dobrać (a,b), aby element $(a-bm,a-b\alpha)\in\mathbb{Z}\times\mathbb{Z}[\alpha]$ był y-gładki

· Niech $U:=\{(a,b):|a|\leqslant u,\ 0<b\leqslant u,\ \mathrm{nwd}(a,b)=1\}$

· Niech $B_1:=\{p:p$ - liczba pierwsza, $\ p\leqslant y\}\cup\{-1\}$

· Używając B_1 można poprzez odsiewanie wyznaczyć podzbiór S takich par $(a,b)\in U$, dla których $(a-bm)$ jest y-gładkie

· Tak wyznaczony zbiór S spełnia warunek (*)

· Znamy wzór na normę, stąd możemy znaleźć te pary (a,b) dla których $N(a-b\alpha)$ jest y-gładka

· Należy zauważyć, że tak uzyskany zbiór nie implikuje (**)

· Będziemy oznaczać $\mathfrak{p}\sim(p,r_p)$ - ideał pierwszy, gdzie $\mathfrak{p}=\ker(\pi)$, dla $\pi:\mathbb{Z}[\alpha]\to\mathbb{F}_p$, natomiast $r_p=\pi(\alpha)$ jest pierwiastkiem wielomianu $(f \bmod p)$

· Definiujemy zbiór $B_2:=\{\mathfrak{p}:\mathfrak{p}\sim(p,r_p),\ p\in B_1\setminus\{-1\},\ r_p\in\mathbb{F}_p\}$

· Używając B_2 można poprzez odsiewanie wyznaczyć podzbiór S' takich par $(a,b)\in U$, dla których $(a-b\alpha)$ jest y-gładkie

· Wyznaczony obszar $U'=S\cap S'$ zawiera takie pary (a,b), że element $(a-bm,a-b\alpha)$ jest y-gładki

· Tworzymy macierz złożoną z wektorów wykładników $(a-bm)$ rozłożonego nad B_1 i $(a-b\alpha)$ nad B_2

· Zależności pomiędzy elementami w powyższej macierzy związane są z podzbiorem $S\subset U'$, dla którego spełnione są dwa warunki:

(+) $\Pi_{(a,b)\in S}(a-bm)$ ma tylko parzyste wykładniki dla wszystkich $p\in\mathbb{Z}$

(++) $\Pi_{(a,b)\in S}(a-b\alpha)$ ma parzyste wykładniki dla wszystkich ideałów pierwszych $\mathfrak{p}\subset\mathbb{Z}[\alpha]$

· Oczywiście z (+) wynika (*). Jednakże istnieją pewne problemy aby z (++) wynikało (**):

- $\mathcal{O}_{\mathbb{Q}(\alpha)}\neq\mathbb{Z}[\alpha]$, wtedy z (++) nie musi wynikać, że $\beta\mathcal{O}$ jest kwadratem jakiegoś ideału

- $\beta\mathcal{O}=\mathfrak{c}^2$, nie oznacza, że $\mathfrak{c}$ jest ideałem głównym

- $\beta\mathcal{O}=\gamma\mathcal{O}$ oznacza tylko, że $\beta=\gamma^2$ z dokładnością do jedności w $\mathcal{O}$

- $\beta=\gamma^2$ w $\mathcal{O}$ nie musi oznaczać, że $\gamma\in\mathbb{Z}[\alpha]$, a jeżeli to nie zachodzi, to γ nie jest argumentem ϕ

Będziemy starać się wyeliminować powyższe problemy poprzez ograniczenie indeksu $[V:(V\cap\mathbb{Q}(\alpha)^{*2})]$ pod-

grupy składającej się z 'właściwych kwadratów' w grupie $V \subset \mathbb{Q}(\alpha)^*$ generowanej przez elementy spełniające (++).

· Niech $\mathcal{O} := \mathcal{O}_{\mathbb{Q}(\alpha)} \subset \mathbb{Q}(\alpha)$ będzie pierścieniem liczb całkowitych.

· Wiemy, że dla $x \in \mathcal{O}$ mamy $f'(\alpha)x \in \mathbb{Z}[\alpha]$

· Wystarczy dla rozwiązania ostatniego problemu aby przypuszczalny kwadrat w $\mathbb{Z} \times \mathbb{Z}[\alpha]$ pomnożyć przez $(f'(m)^2, f'(\alpha)^2)$

· Warunkiem, dla którego powyższy sposób jest skuteczny jest gdy $f'(m)$ jest względnie pierwsze z n. Jeżeli tak nie jest - znaleźliśmy nietrywialny dzielnik n

· $\mathbb{Q}(\alpha)^*$ jest generowane przez elementy $a - b\alpha \in \mathbb{Z}[\alpha]$, takie że $\text{nwd}(a, b) = 1$

· Mamy $V \subset \mathbb{Q}(\alpha)^*$ zawierający elementy mające parzyste wykładniki dla wszystkich ideałów pierwszych $\mathfrak{p}$ w $\mathbb{Z}[\alpha]$

· Rozpatrzmy $V_1 \subset V$ złożony z elementów $x \in V$, które mają parzyste wykładniki dla ideałów pierwszych $\mathfrak{q}$ w $\mathcal{O}$, np. w V_1 są te $x \in V$, dla których $x\mathcal{O}$ jest kwadratem pewnego ideału z $\mathcal{O}$

· Budując odpowiednie zanurzenie oraz korzystając z faktu, że $[\mathcal{O} : \mathbb{Z}[\alpha]] \leqslant |\Delta(f)|^{\frac{1}{2}}$ możemy oszacować $dim(V/V_1) \leqslant \frac{d}{2} \log \Delta(f)$

· Jest to pierwszy krok do sukcesywnego ograniczania wymiaru, gdyż $V \supset V_1 \supset V_2 \supset V_3 = V \cap \mathbb{Q}(\alpha)^{*2}$

· V_2 jest podgrupą tych $x \in V$, dla których $x\mathcal{O}$ jest kwadratem ideału głównego w $\mathcal{O}$

· Możemy oszacować liczbę klas $h \leqslant |\Delta(f)|^{\frac{1}{2}} \frac{d-1+\log |\Delta(f)|^{d-1}}{(d-1)!}$

· Dla takiego oszacowania mamy, że $dim(V_1/V_2) \leqslant \frac{\log h}{\log 2}$ oraz $dim(V_2/V_3) \leqslant d$

· Ostatecznie otrzymujemy, że dla $1 < d^{2d^2} < n$ mamy następujące oszacowanie $dim(V/V_3) \leqslant (\log n)^{\frac{3}{2}}$

· Przedstawiony wcześniej algorytm pozwala nam działać na elementach z $\mathbb{Z} \times \mathbb{Z}[\alpha]$ takich, że drugi element należy do V, jednak nie mamy pewności, że należy do V_3

· Należenie elementu $x \in V$ do V_3 jest tożsame z tym, że wszystkie charaktery $\chi : V/V_3 \to \mathbb{F}_2$ znikają na x.

· Nie musimy jednak sprawdzać wszystkich charakterów, gdyż najwyżej $k = dim(V/V_3)$ jest potrzebnych do rozpięcia przestrzeni wszystkich homomorfizmów z V/V_3 do $\mathbb{F}_2$

· Jeżeli dla $x \in V$ każdy z tych najwyżej k charakterów przyjmuje wartość 1 to x jest kwadratem

· Nie jest łatwo wybrać taki zbiór charakterów, dlatego przyjmiemy losowy zbiór charakterów kwadratowych

· Jeżeli wybierzemy losowo $k + e$ charakterów to szansa, że znajdziemy wśród nich odpowiednie k charakterów wynosi $1 - 2^{-e}$

· Dla $x \in \mathbb{Z}$ możemy zastosować symbol Legendre'a - jeżeli dla t losowo wybranych liczb pierwszych p zachodzi

$(\frac{x}{p}) = 1$, to x jest kwadratem z prawdopodobieństwem $1 - 2^{-t}$.

· Chcielibyśmy przeprowadzić podobne rozumowanie dla $x \in \mathbb{Z}[\alpha]$

· Dla każdego ideału pierwszego $\mathfrak{q} \sim (q, r_q)$ konstruujemy symbol Legendre'a następująco:

$(\frac{\cdot}{\mathfrak{q}}) : \mathbb{Z}[\alpha] \xrightarrow{\pi} \mathbb{F}_q \xrightarrow{(\frac{\cdot}{q})} \{\pm 1\} \cup \{0\}$

· Jeżeli x jest y-gładkie, to unikamy wartości 0 dla $q > y$

· Jeżeli $(\frac{x}{\mathfrak{q}}) = -1$ dla więcej niż połowy przypadków, stwierdzamy że x nie jest kwadratem w $\mathbb{Z}[\alpha]$

· Do B_1 oprócz liczb pierwszych włączyliśmy $\{-1\}$, analogicznie do B_2 dołączamy zbiór charakterów $\chi_{\mathfrak{q}} : V \to \mathbb{F}_2$ związanych z $(\frac{\cdot}{\mathfrak{q}})$

· Stworzyliśmy probabilistyczny algorytm wybierania y-gładkich $x \in V$, które nie tylko spełniają (++), ale także są 'właściwymi kwadratami'.

· Przy tak przesianych wartościach (a,b) mamy, że $\left(f'(m)^2 \, \Pi_{(a,b)\in S} \, (a - bm), \; f'(\alpha)^2 \, \Pi_{(a,b)\in S} \, (a - b\alpha) \right)$ jest z dużym prawdopodobieństwem kwadratem (x^2, β^2) w $\mathbb{Z} \times \mathbb{Z}[\alpha]$

· Mając (x^2, β^2) chcielibyśmy uzyskać $(x \bmod n)$ oraz $\phi(\beta)$, gdyż ich różnica jest nietrywialnym dzielnikiem n.

· Możliwe jest szybkie obliczenie $(x \bmod n)$ nawet dla dużych wartości $x^2 = f'(m)^2 \Pi_{(a,b)\in S}(a - bm)$, o ile znamy rozkład na czynniki każdego z elementów $(a - bm)$.

· Dlatego najpierw dla elementów $(a - bm)$ stosujemy odpowiednie metody faktoryzacji (zależne od postaci tych elementów)

· Jeżeli $\mathbb{Q}(\alpha)$ nie jest odpowiednie, to ciężkim zadaniem stanie się policzenie grupy jedności $\mathcal{O}^*$

· Jedynie dla pierścienia liczb całkowitych, dla którego mamy małą grupę jedności i trywialną grupę klas jesteśmy w stanie w rozsądnym czasie wyliczyć pierwiastek z β^2

· Ogólnie możemy policzyć pierwiastki $X^2 - \beta^2$ w $\mathbb{Q}(\alpha)$ korzystając z lematu Hensela, bądź metody Montgomery'ego

· Po uzyskaniu wartości $(x \bmod n)$ oraz $\phi(\beta)$ liczymy ich różnicę i otrzymujemy nietrywialny pierwiastek n.

Bibliografia

[1] A. Lenstra and H.W.J.(eds) Lenstra, *The develompemnt of the number field sieve*, Lecture Notes in Mathematics, vol. 1554, Springer - Verlag, 1993.

[2] P.W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, Journal on Scienrific Computing **26** (1997).

[3] P. Stevenhagen, *The number field sieve*, Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, 2005.