RSA κρυπτγράφηση και ο κβαντικός αλγόριθμος του Shor για αποκρυπτογράφηση

Γεώργιος Κυριάκου, ΤΗΜΜΥ ΑΠΘ, Μάιος 2017

krkgeorge1995@gmail.com

- Μέθοδος προστασίας των δεδομένων επικοινωνίας με την εφαρμογή μετασχηματισμών υπολογιστικά απλών ευθέως, αλλά δαπανηρών αντιστρόφως
- Δημοφιλής η χρήση εκφράσεων με πρώτους (prime) αριθμούς
- Σχετικοί αλγόριθμοι: Cock, RSA

Βασική ιδέα: αν N=p·q πολύ μεγάλος ακέραιος, η εύρεση των πρώτων παραγόντων p, q είναι υπολογιστικά αδύνατη με απλές μεθόδους

Τι είναι/πως λειτουργεί η κρυπτογράφηση;

- Κρυπτογράφηση: $C = (M^e) \, mod \, n$
- Αποκρυπτογράφηση: $M = \left(C^d\right) mod \, n$

M,C τα μηνύματα πριν και μετά την κρυπτογράφηση
N ένας μεγάλος ακέραιος (πχ 128 bit) ως γινόμενο primes

Τα ζεύγη (n,e) και (n,d) είναι το δημόσιο και το ιδιωτικό κλειδί.

Ισχύει (αλγόριθμος Euler): $e \cdot d \, mod \, (p-1) \cdot (q-1) = 1$

Πως πραγματοποιείται η κρυπτογράφηση/αποκρυπτογράφηση RSA;

Από τη θεωρία αριθμών…

- Στο διάστημα (0,N) υπάρχουν κατά προσέγγιση N/(ln(N)) πρώτοι αριθμοί
- Όταν ψάχνουμε τους πρώτους παράγοντες σύνθετου αριθμού N, αρκεί να εξετάσουμε μέχρι το $\sqrt{N}$

Άρα η πολυπλοκότητα του απλούστερου (brute-force) αλγορίθμου θα είναι $O\left(\frac{\sqrt{N}}{\ln(\sqrt{N})}\right) = O\left(\frac{2\sqrt{N}}{\ln(N)}\right)$ (μικρότερη από O(N))

Ευτυχώς για μας, μπορεί να μειωθεί κι άλλο!

Ποιά είναι η πολυπλοκότητα/μπορεί να μειωθεί;

1. Διαλέγουμε έναν αριθμό $\alpha \leq \sqrt{\mathrm{N}}$. Εξασφαλίζουμε ότι τα α, Ν είναι πρώτοι μεταξύ τους, δηλαδή ΜΚΔ(α,Ν)=1
2. Βρίσκουμε την περίοδο r . Ορίζεται ως ο πρώτος αριθμός έτσι ώστε $\alpha^r \ mod \ N = 1$
3. Βασική σχέση: $\left(\alpha^{r/2}+1\right)\cdot\left(\alpha^{r/2}-1\right)=\mathrm{k}\cdot N$, k ακέραιος. Αν $\left(\alpha^{r/2}+1\right) mod \ N = 0$, πρέπει να βρούμε άλλο α
4. Τότε $p = \mathrm{ΜΚΔ}\left(\alpha^{r/2}-1,\mathrm{N}\right)$ και $p = \mathrm{ΜΚΔ}\left(\alpha^{r/2}+1,\mathrm{N}\right)$

Ταχύτερος Αλγόριθμος (Shor) για την εύρεση των p, q

- Όλα τα βήματα μας είναι απλά υπολογιστικά (ο ΜΚΔ υπολογίζεται με τον Ευκλείδειο αλγόριθμο)
- Η δυσκολία ανάγεται στον υπολογισμό της περιόδου r

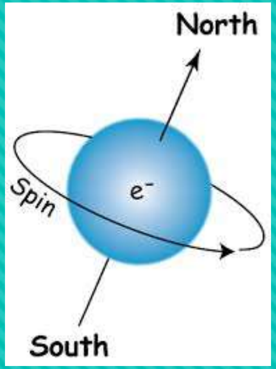
Ο RSA λειτουργεί αποτελεσματικά επειδή για να βρούμε το r, πρέπει να εξετάσουμε και πάλι ενα μεγάλο πλήθος αριθμών (εκθετικό ως προς τα bit)

Το μεγάλο πλεονέκτημα είναι η απλή υλοποίηση του βήματος αυτού σε κβαντικό υπολογιστή!

Τι πετύχαμε;

- Βασική μονάδα όχι το bit, αλλά το qubit
- Τα qubit παίρνουν τις τιμές 0 και 1 κάθε φορά που παρατηρείται το αποτέλεσμα μιας πράξης
- Τα qubit βρίσκονται σε υπέρθεση άπειρων καταστάσεων μεταξύ 0 και 1 (superposition), που περιγράφεται απο μία pdf ενόσω εκτελούν υπολογισμούς

Κλασικότερη φυσική υλοποίηση: ηλεκτρονιακό σπιν



Τι είναι ο κβαντικός υπολογιστής/Πώς λειτουργεί;

Λίγα χρήσιμα μαθηματικά σύμβολα...

1. *Η κατάσταση ενός qubit θεωρείται διάνυσμα $|y\rangle$ στον $\mathbb{C}^{2^n}$ (για n qubits)*
2. *Η υπέρθεση καταστάσεων περιγράφεται ως διάνυσμα σε ένα χώρο με βάση τις 2^n διαφορετικές δυνατές καταστάσεις*
   $$|y\rangle = \sum_{i=0}^{2^n-1} a_i |S_i\rangle$$
3. *Οι δυνατοί υπολογισμοί (πύλες) αναπαρίστανται ως ορθομοναδιαίοι (unitary) πίνακες (δηλαδή ισχύει $\boldsymbol{U}^H = \boldsymbol{U}^{-1}$)*

Σημαντικό: Η ποσότητα a_i^2 είναι η πιθανότητα παρατήρησης της κατάστασης $|S_\mathrm{i}\rangle$

Κβαντική λογική/Κβαντικές πύλες και μαθηματική αναπαράσταση

Αρχική κατάσταση $\|0\rangle$ - *πύλη Hadamard* $= \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$		
$\frac{1}{\sqrt{2}}\|0\rangle$	$+$	$\frac{1}{\sqrt{2}}\|1\rangle$

Πύλη Pauli-Y $= \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$		
$\frac{i}{\sqrt{2}}\|1\rangle$	$+$	$-\frac{i}{\sqrt{2}}\|0\rangle$

Πύλη Pauli-X (NOT) $= \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$		
$\frac{i}{\sqrt{2}}\|0\rangle$	$+$	$-\frac{i}{\sqrt{2}}\|1\rangle$

Ένα απλό παράδειγμα

- Η κβαντική υπέρθεση επεξεργάζεται 2^n καταστάσεις ταυτόχρονα
- Ν κβαντικές πύλες = 2^n ψηφιακές πύλες
- Πάντα τρέχουμε τους κβαντικούς αλγορίθμους πάνω άπο μία φορά (η παρατήρηση αποτελέσματος εμπλέκει πιθανότητα)

Στόχος: Να εφαρμόσουμε εκείνο το μετασχηματισμό (πύλες) που μεγιστοποιούν την πιθανότητα παρατήρησης της σωστής κατάστασης (δηλαδή τα p, q)

Και ποιός είναι ο κατάλληλος μετασχηματισμός; Wait for it…

Πως βελτιώνει ο κβαντικός υπολογιστής την πολυπλοκότητα;

Δεδομένων των N (μέγεθος) και α (είσοδος) σε δυαδική μορφή, ο QFT ορίζεται ως:

$$\hat{\alpha} = \frac{1}{\sqrt{N}} \sum_{\psi=0}^{N} |\psi\rangle e^{\frac{2\pi i a \psi}{\mathrm{N}}}$$

- Γρήγορος υπολογισμός μέσω του κβαντικού FFT
- Χρησιμοποιεί $l \cdot (l-1)/2$ κβαντικές πύλες, όταν $\mathrm{N} = 2^l$
- Περιγράφεται συνολικά από τον unitary πίνακα A_N, για τον οποίο ισχύει $(A_N)_{a\psi} = \frac{1}{\sqrt{N}} e^{\frac{2\pi i a \psi}{\mathrm{N}}}$

Ο κβαντικός μετασχηματισμός Fourier! (QFT)

1. Χρησιμοποιούμε 2 κβαντικούς καταχωρητές
2. Διαλέγουμε ένα q τέτοιο ώστε $N^2 \leq q \leq 2N^2$
3. Ο πρώτος καταχωρητής τίθεται σε κατάσταση με βάση τα διανύσματα $|\mathrm{r}\ mod\ q\ \rangle$, και ομοιόμορφη κατανομή
4. Ο δεύτερος καταχωρητής, τίθεται σε κατάσταση με βάση τα $|\mathrm{r}\ \rangle|(\alpha^r)\ mod\ N\rangle$ και ομοιόμορφη κατανομή. Εδώ χρησιμοποιούνται τιμές του πρώτου καταχωρητή
5. Εφαρμόζουμε A_q QFT στον πρώτο καταχωρητή
6. Παρατηρούμε τις τιμές στους καταχωρητές. Αναμένουμε να παρατηρήσουμε την περίοδο r στον πρώτο, και 1 στον δεύτερο

Πως εφαρμόζεται αύτη η ιδέα στον αλγόριθμο του Shor;

- Η εύρεση του r γίνεται σε πολυωνυμικό χρόνο καθώς εφαρμόζεται πολυωνυμικής τάξης πλήθος πυλών για τον QFT όπως επίσης και για την υπέρθεση στους καταχωρητές
- Η πολυπλοκότητα αποδεικνύεται ότι μειώνεται ακολούθως στο $O((\log N)^2 \cdot loglog(N) \cdot logloglog(N))$

Δεν ξεχνάμε: ο αλγόριθμος Shor δεν είναι πάντα ακριβής, αλλά έχει αποδειχθεί ότι η λύση βρίσκεται πάντα κοντά στην παρατηρούμενη τιμή

Τι καταφέραμε;

- Το 2001 η IBM πέτυχε την πρώτη υλοποίηση παργοντοποιώντας το 13, με NMR (Nuclear Magnetic Resonance)
- Οι επόμενες υλοποιήσεις επιτεύχθηκαν με photonic qubits
- Το 2012 παραγοντοποιήθηκε το 21 εγκαθιδρύοντας το σημερινό ρεκόρ

- Βασική δυσκολία η απαλοιφή του θορύβου μετρήσεων
- Απαιτητική η κβαντική αποσύμπλεξη καταστάσεων (quantum decoherence)
- Για μεγάλο μέγεθος παρουσιάζονται ασταθείς συμπεριφορές

Υλοποιήσεις/Δυσκολίες

Ευχαριστώ πολύ για την προσοχή σας!

https://www.youtube.com/watch?v=IrbJYsep45E
https://www.youtube.com/watch?v=12Q3Mrh03Gk
https://www.youtube.com/watch?v=wUwZZaI5u0c