Populärvetenskaplig sammanfattning

Erik Mårtensson

2020–12–17

Att kunna skicka krypterade meddelanden är inte längre bara angeläget för militärer och underrättelsetjänster. Varje gång du betalar räkningar via din internetbank eller handlar varor över internet vill du kryptera meddelanden du sänder så att inte obehöriga kan ta del av känslig information.

Symmetrisk kryptering

Tänk dig situationen att Alice vill skicka ett hemligt meddelande till Bob. Inom det som kallas symmetrisk kryptering använder Alice då ett hemligt ord (nyckel) för att göra meddelandet oläsligt (kryptera). Bob använder sen samma nyckel för att göra det krypterade meddelandet läsligt igen (dekryptera). Med symmetrisk kryptering kan stora mängder data skickas snabbt och säkert. Ett problem är dock hur Alice och Bob ska komma överens om en gemensam nyckel. Ett sätt detta kan göras på är med asymmetrisk kryptering.

Asymmetrisk kryptering

Inom asymmetrisk kryptering har Bob två nycklar, en publik nyckel som vem som helst kan se och en privat nyckel som bara Bob kan se. Alice skickar nu ett krypterat meddelande med hjälp av Bobs publika nyckel. Bob dekrypterar sen meddelandet med hjälp av sin privata nyckel.

Kvantdatorer

För att kunna dekryptera meddelandet utan tillgång till den privata nyckeln måste en attackerare lösa ett matematiskt problem. Kryptering idag är baserat på att det är svårt att faktorisera väldigt stora tal eller att hitta diskreta logaritmer i ändliga grupper. Trots decennier av intensiv forskning har ingen lyckats hitta effektiva algoritmer för att lösa dessa problem med en klassisk dator.

En klassisk dator arbetar med bitar, som kan anta värdet 0 eller 1. Ett register med n bitar kan i sin tur vara i något av 2^n tillstånd. En kvantdator

är en dator baserad på kvantbitar, där n kvantbitar befinner sig i superposition mellan dessa 2^n tillstånd. När man mäter tillståndet på kvantbitarna kollapsar dessa till ett av de 2^n tillstånden. Kvantalgoritmer applicerar unitära transformationer på kvantbitarna på ett sätt så att sannolikheten är hög att dessa kollapsar till rätt tillstånd när man väl gör en mätning.

Med hjälp av Shors algoritm kan kvantdatorer både faktorisera tal och hitta diskreta logaritmer på ett effektivt sätt. Idag kan kvantdatorerna bara hantera ett fåtal kvantbitar. Men får vi storskaliga kvantdatorer i framtiden visar det sig att det är lätt att faktorisera stora tal och då behöver vi basera kryptering på andra matematiska problem.

Postkvantkryptering

Forskningsområdet där man studerar ersättare till dagens system för asymmetrisk kryptering kallas postkvantkryptering. Två av huvudspåren inom postkvantkryptering är gitterbaserad kryptering och kodbaserad kryptering.

Gitterbaserad kryptering

Ett gitter i tre dimensioner beskriver den diskreta placeringen av atomer i en kristallstruktur. Matematiskt kan man generalisera denna struktur till godtyckligt antal dimensioner. I högre dimensioner visar det sig vara ett svårt problem att, givet en godtycklig punkt, hitta den närmaste gitterpunkten. Gitterbaserad kryptering är baserad på att detta problem är svårt. I artikel 3 studerade vi hur algoritmer för att lösa detta problem kan förbättras med hjälp av en kvantdator.

LWE

Att lösa linjära ekvationssystem med tusentals ekvationer och obekanta är enkelt för en modern dator. Learning with Errors (LWE) är en variant av detta problem, men med små brustermer tillförda varje ekvation. Ett sätt att lösa LWE på är att översätta problemet till att leta efter den närmaste punkten i ett gitter.

En annan typ av algoritm kallas Blum-Kalai-Wasserman (BKW) och innebär en generalisering av Gausselimination, som används för att lösa brusfria, linjära ekvationssystem. Artikel 1, 2, 5 och 6 handlar om olika aspekter av denna typ av algoritm, från olika tekniker för att förbättra algoritmen till implementering av algoritmen för att lösa konkreta instanser av LWE.

Kodbaserad kryptering

Kodbaserad kryptering använder tekniker från felkorrigerande koder för att kryptera meddelanden. Alice transformerar sitt meddelande till ett kodord i en linjär kod. Sen lägger hon medvetet på nog med brus till meddelandet så att det blir oläsligt för attackeraren. Bob har hemlig tillgång till den linjära kodens struktur och kan med hjälp av denna korrigera bort bruset och på så sätt läsa meddelandet. Normalt används binärt brus (0:or och 1:or). I artikel 4 studerade vi vad som händer om man istället använder normalfördelat brus och visade att detta leder till allvarliga sårbarheter. Algoritmen vi utvecklade för att lösa detta problem visade sig ha applikationer även inom andra områden av kryptering och inom kodningsteknik.