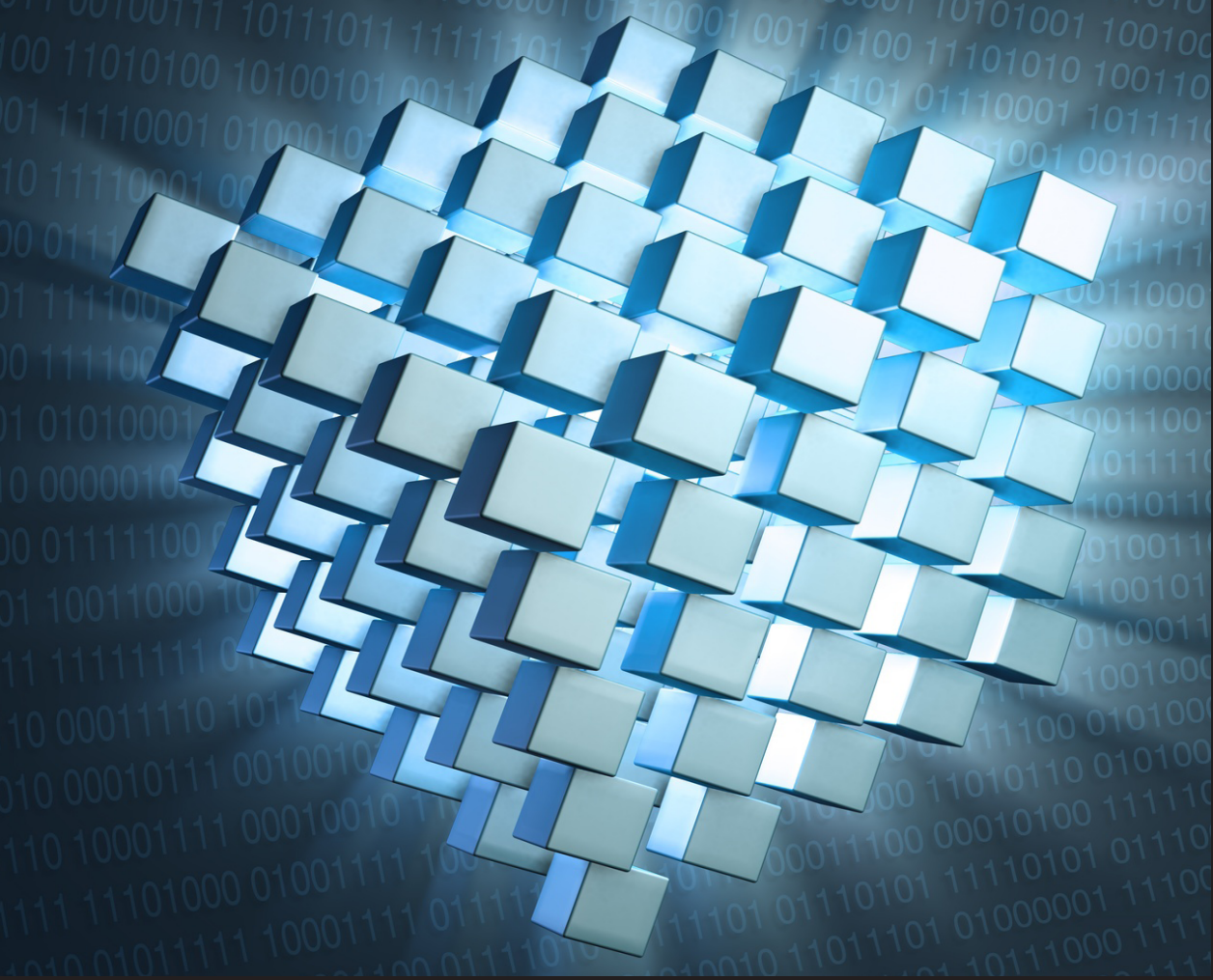


Kvantinformatik

Elias Amselem, Pontus Svenson, Linus Gisslén

FOI-R--3920--SE

Augusti 2014

FOI

Elias Amselem,Pontus Svenson,Linus Gisslén

Kvantinformatik

Bild/Cover: Pixtal/TT.se

FOI-R--3920--SE

Titel	Kvantinformatik
Title	Quantum Information
Rapportnr/Report no	FOI-R—3920--SE
Månad/Month	Aug
Utgivningsår/Year	2014
Antal sidor/Pages	54 p
ISSN	1650-1942
Kund/Customer	FMV
Forskningsområde	1. Beslutsstödssystem och informationsfusion
FoT-område	Avskanning av forskningsfronten
Projektnr/Project no	E34220
Godkänd av/Approved by	Lars Höstbeck
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Kvantinformatik är ett tvärvetenskapligt ämne där kvantfysik möter informationsteori. Två delar inom ämnet, kvantkryptografi och kvantdatorn, är mer applikationsinriktade och kan potentiellt ha stora konsekvenser för samhälle, försvar och säkerhet. Rapporten fokuserar på att ge en överblicksbild där vi belyser statusen idag, pågående teknikutveckling och prognoser över vilka medel som kommer kunna var tillgängliga i framtiden.

Kvantfysikens stokastiska natur med dess kopieringsrestriktioner möjliggör distribution av korrelerade slumptalslistor, dvs. en krypteringsnyckel, mellan flera parter. Samtidigt fås möjligheten till en flaggning av en potentiell avlyssning i kommunikationslinan. Idag finns flera företag som säljer kvantkrypteringsutrustning och insatser görs i flera länder för att bygga upp kvantvänliga fibernätverk. Uppskjutningen av en satellit är även planerad för att möjliggöra distribution av kvantmekaniskt korrelerade ljuspartiklar (fotoner) över stora avstånd.

Kvantdatorn ska inte förväxlas med en superdator som förknippas med extra många beräkningar per sekund. Kvantdatorn är något helt nytt där effektiviteten kommer av att den löser problem genom att utnyttja nya beräkningsmöjligheter som inte är tillgängliga för en klassisk datorarkitektur. Dessa uppkommer eftersom den bearbetar ettor och nollor genom ett kvantmekaniskt regelverk. Förmågor som den förväntas ha är bland annat effektiva simuleringar av kvantmekaniska effekter, avancerade sökningar i stora databaser och bryta eller försvaga flera populära krypteringsmetoder. Idag sker en kapplöpning där ett stort antal olika teknologier har potentialen till förverkligandet. Endast ett fåtal kvantmekaniska ettor och nollor kan idag med säkerhet realiseras och forskargrupper försöker nu skala upp experimenten. Trots den låga mognadsgraden finns det djärva men hårt kritiserade företaget D-wave som redan idag påstår sig kunna bygga en kvantdator som Google, NASA och Lockheed Martin investerat i.

Nyckelord: Kvantdator, kryptografi, kvantinformatik, kvantalgoritmer, kvantkommunikation, kvantkrypton

Summary

Quantum information is an interdisciplinary field where quantum physics meets information theory. Quantum cryptography and quantum computing are the two parts that are more application-oriented and can potentially have a major impact on society, defense and security. The report focuses on providing an overview where we highlight the status today, ongoing technology development and forecasts of the technologies that might be available in the future.

The stochastic nature of quantum physics together with the information cloning restriction enable the distribution of correlated random lists, i.e. an encryption key, between multiple parties. At the same time it is possible to obtain a warning of a potential eavesdropper in the communication line. Today there are several companies selling quantum cryptography equipment and efforts are being made in several countries to build quantum friendly fiber networks. A satellite launch is also planned to allow for the distribution of quantum correlated light particles (photons) over large distances.

The quantum computer should not be confused with a supercomputer which is associated with many calculations per second. Instead it is something completely new where the efficiency comes from the ability to solve problems by using new computing methods that are not available with classical computer architecture. These new methods arise because it manipulates ones and zeros by a quantum mechanical framework. Expected is that it will be able to help in effective simulations of quantum effects, advanced searches of large databases and break or weaken several popular encryption methods. Today, a large number of different technologies are potential candidates. But until now only a few quantum mechanical ones and zeros has been demonstrated and research groups are trying to scale up experiments. Despite the low level of maturity there is D-wave which is a criticized company that already claims to be able to build a quantum computer. Despite the critics Google, NASA and Lockheed Martin have invested in the company.

Keywords: quantum information, quantum computing, quantum key distribution

Innehållsförteckning

1 Inledning

Kvantinformatik är ett relativt nytt ämne som har sina rötter i fysikens värld. Under början av 1900-talet presenterades flera nya koncept inom fysiken som slutligen kulminerade med den kvantmekaniska teorin. Trots sina stora framgångar att förutsäga experimentella resultat startade en debatt om hur väl teorin egentligen speglar verkligheten. Debatten kretsade kring att den kvantmekaniska teorin har flera svårsmälta ingredienser i sig som strider mot den klassiska världsbild vi är vana vid. Dessa fenomen, till exempel superpositionsprincipen (saker och ting kan befinna sig på flera ställen samtidigt), vågpartikeldualismen (partiklar beter sig som vågor och vågor som partiklar) och snärjelse (starka korrelationer mellan partiklar), kom att visa sig ha stor potential inom både kryptografi och datavetenskap.

Den tidiga debatten berörde framförallt den grundläggande fysiken. Men med den alltmer accelererande utvecklingen inom den klassiska informationsteknologin började fysiker att resonera i termer av informationsteori och informationsteknologi. År 1959 höll Richard Feynman sitt berömda tal ”there is plenty of room at the bottom” där han manade fysiksamfundet att börja betrakta kvantmekaniska effekter för att designa kretsar och instrument med helt nya egenskaper.

> ”When we get to the very, very small world, say, circuits of seven atoms, we have a lot of new things that would happen that represent completely new opportunities for design. Atoms on a small scale behave like nothing on a large scale, for they satisfy the laws of quantum mechanics. So, as we go down and fiddle around with the atoms down there, we are working with different laws, and we can expect to do different things. We can manufacture in different ways. We can use not just circuits but some system involving the quantized energy levels, or the interactions of quantized spins, etc.”[a,b]

Fältet kvantinformatik har sedan dess växt och i dagsläget är vissa delar på väg mot kommersialisering. Drivkrafterna har varit flera där ett argument är bland annat Feynman’s [1] insikt om att simuleringar av kvantfenomen troligen tar så lång tid att de ofta inte är praktiskt genomförbara varken på dagens eller på framtida klassiska datorer. Denna idé vidareutvecklades av David Deutsch till teorin om den universella kvantdatorn [2]. Senare, år 1996, visade Seth Lloyd

[a] Hela talet kan läsas på: www.zyvex.com/nanotech/feynman.html .
[b] Bild från: en.wikipedia.org/wiki/Richard_Feynman

teoretiskt att lokala kvantmekaniska system kan simuleras effektivt av en kvantdator [3]. Att effektivt kunna simulera kvantmekaniska system har stor potential för tillämpning i bland annat områden som utvecklingen av nya material, beräkning av materialegenskaper, kemiska egenskaper, optiska egenskaper och mekaniska egenskaper. Andra framsteg förutom effektiva simuleringsmetoder för kvantmekaniska system är:

- Skapandet av kvantkryptografin som kan garantera krypteringssäkerhet via fysikens lagar.
- Shors faktoriseringsalgoritm som har potential att kunna bryta dagens RSA-krypteringssystem på några minuter.
- Grovers sökalgoritm som skulle kunna försvaga säkerheten i det mycket populära AES-krypteringssystemet.

Det kan tyckas att genombrotten är få och vaga men de väger tungt på grund av deras potentiella inverkan på säkerhetsområdet och framförallt för att detta troligen bara är toppen av kunskapsberget som än inte är utforskat. Förväntan på kvantinformatik kan, till viss del, liknas till datorn som en gång i tiden antogs vara ett begränsat instrument som aldrig skulle nå den breda massan, men idag ser vi att den har förändrat världen på ett sätt som ger ett intryck av att mänskligheten nästintill inte kan leva utan den. Kvantinformatikens riktiga potential och förmåga kommer bara att ses när forskare och ingenjörer har tillgång till kvantdatorn.

De redan idag kända användningsområdena har potential att få stor samhällspåverkan när/om de blir möjliga att realisera. En av de stora styrkorna som kvantdatorn förväntas ha är möjligheten att söka och hitta mönster i stora och komplexa datamängder. Därför förväntas applikationer riktade mot artificiell intelligens, sökmotorer, igenkänning, simuleringar där många val måste bearbetas (till exempel i vädersimuleringar), genetik och materialforskning. Det finns också vissa indikationer på att naturen själv använder sig av kvantinformationskoncept för att optimera och förstärka vissa processer, t.ex. finns bevis att en form av kvantmekanisk slumpvandring[c] sker i fotosyntesen. Dessutom finns indikationer på att vissa arter av duvor har förmåga att känna av riktningen på jordens magnetfält då de exponeras av blått eller grönt ljus men förlora förmågan då exponeringen är rött ljus[d]. Förmågan anta uppstå genom att en ljuspartikel exitetrar en molekyl som skapar ett starkt korrelerat kvantmekaniskt tillstånd, kallas även för ett snärjat tillstånd, mellan molekylens

[c] Kvantmekanisk version av slumpvandring där partiklar kan med en viss sannolikhet hoppa från en position till en annan och på så sätt sprida ut sig för att testa många olika vägar genom kloroplasten som finns i växtcellen.

[d] Se MIT professorns Seth Lloyds föredrag ”Seth Lloyd on quantum life”: www.youtube.com/watch?v=wcXSpXyZVuY

partiklar. Det snärjda tillståndet förväntas vara mycket känsligt för magnetfältets riktning. Rött ljus som har lägre energi än de blåa kan inte excitera molekylen som är inblandad i processen.

Viktigt att förstå är att kvantdatorn må vara ett attraktivt mål men även forskning som leder dit skapar ständigt nya teknologier. Redan i dag ser vi många teknologier som i grunden baserar sig på koherent kontroll[e] och representerar de första stegen mot storskalig kontroll av partiklar. Några exempel är lasern, medicinsk avbildning via kärnmagnetisk resonans (NMR/MRI), elektronspinn resonans (ESR/EPR), atomur för exakt tidmätning (används i bland annat GPS satelliter), atominterferometrar (för exempelvis precisionsmätningar av gravitationen, acceleration och rotationer) och fotonräknande detektorteknologier som SSPD (Superconducting single photon detectors). Det här är bara några få exempel på teknologier som har uppkommit tack vare forskning som strävar efter koherent kontroll av partiklar.

I föreliggande rapport beskrivs de delar av kvantinformationsfältet som är relaterat till kvantkryptografi och kvantdatorer. Syftet är att ge läsaren en inblick i de olika teknikerna, framstegen, potentialen, och dess begränsningar. Under skrivandets gång har vi försökt att hålla matematiken på en minimal nivå, men dessvärre är ämnet hårt knutet till fundamental fysik och informationsteori vilket innebär att vissa koncept inte alltid går att beskriva på ett enkelt sätt. Rapporten är strukturerad så att de viktigaste koncepten för grundläggande kvantinformatik introduceras i kapitel 1 och ligger till grund för resterande delar. I kapitel 1.1 ges en snabb överblick av de viktigaste koncepten i punktform för att ge en grund till ämnet som behandlas innan vi går in i varje ämne var för sig. Kärnan i rapporten är kapitel 2 och 3 där vi behandlar kvantkryptografi (2) och kvantdatorer (3). Rapporten avslutas med kapitel om bevakningsbehov (4) och säkerhetsaspekter på kvantinformatik (5). Kapitlet om säkerhetsaspekter sammanfattar innehållet av förgående kapitel genom att ge prognoser om hur området kvantinformatik kan tänkas utvecklas.

1.1 En kort överblick

Innan vi går in i detalj i varje ämne vill vi ge en överblick genom att gå igenom vanliga frågor som ofta uppkommer.

VAD ÄR EN DATOR? En maskin som bearbetar ettor och nollor enligt ett regelverk. Detta regelverk baserar sig på klassisk fysik dvs. fysiken som uppkom innan 1900-talet. Varje instruktion tar en given kombination av ettor och nollor som matas in en i taget. För att utföra många olika instruktioner måste varje kombination utföras i serie en efter en. Alla typer av dagens konventionella

[e] Se avsnitt 1.2.1, koherens kan ses som förmågan att kunna sätta atomer i och bevara en superposition. (http://www.ne.se/lang/koherens)

datorer fungera enligt denna princip oavsett om det är en mobiltelefon eller en superdator.

VAD ÄR KVANTFYSIK? En teori inom fysiken som beskriver små och isolerade system, exempel på kvantmekaniska system är atomer och andra fundamentala partiklar. Kvantfysiken har haft mycket stora framgångar i att förutsäga experimentella resultat. Teorin kan verka kontraintuitiv och innehåller idéer där partiklar kan befinna sig på flera platser samtidigt (superposition) och effekter som kvantteleportering där information kan flyttas genom en viss typ av kvantmekaniska korrelationer (även kallat snärjelse) mellan partiklarna.

VAD ÄR KVANTKRYPTOGRAFI? En metod som använder kvantmekanikens lagar för att överföra slumptal mellan flera parter via t.ex. optiskfiber eller satellit så att det är teoretiskt omöjligt att avlyssna överföringen utan att upptäckas. Slumptalen används sedan som krypteringsnycklar för att låsa meddelanden. Främst är kvantkryptografi en metod för att distribuera krypteringsnycklar där säkerheten baserar sig på fysikens lagar och inte på svåra beräkningar som är grunden till dagens krypteringstekniker.

VAD ÄR EN KVANTDATOR? En maskin som bearbetar ettor och nollor genom ett kvantmekaniskt regelverk där superposition och snärjelse har viktiga roller. Regelverket och fysiken i kvantdatorn är fundamentalt annorlunda jämfört med en klassisk dator. Detta medför att kvantdatorn kan utföra vissa saker som en klassisk dator har mycket svårt att utföra. Kvantdatorns effektivitet kommer inte av att den gör fler beräkningar per sekund utan istället löser den problemen genom att utnyttja lösningsmetoder, via kvantfysiken, som inte är tillgängliga för en klassisk dator.

VAD KAN MAN GÖRA MED EN KVANTDATOR? Detta är en svår fråga och beror på vilken typ av kvantdator som kommer att vara tillgänglig. Men förväntningen är att simuleringar av komplexa kvantmekaniska system kommer att var den dominerande applikationen till en början. Detta kommer troligtvis skapa genombrott i flera forskningsfält där simuleringar är begränsningen i dag. Kvantdatorn kommer troligtvis ha applikationer inriktade mot komplexa sökningar i stora databaser, igenkänning, simulering av väder, genetik och materialforskning. Förutom simuleringar har kvantdatorn även potential att bryta eller försvaga säkerheten på flera mycket populära krypteringsmetoder. Denna applikation är kanske den mest omtalade eftersom ett förverkligande skulle ha stor påverkan på internetsäkerheten. Att effektivt simulera kvantmekaniska effekter, och bryta eller försvaga flera populära krypteringsmetoder är några uppgifter som inte kan utföras effektivt på dagens datorer.

KAN MAN BYGGA EN KVANTDATOR? Ingen storskalig maskin har ännu byggts utan bara system som kan hantera ett fåtal kvantmekaniska ettor och nollor har demonstrerats. Precis som när datorer kom så är dagens kvantdatorer stora och högspecialiserade för vissa problemtyper. De kommer att ha de

negativa egenskaperna tills teknologiska genombrott kan förminska storleken och generalisera problemtyperna. Idag finns många olika teknikkandidater och alla har sina fördelar och nackdelar. Stora forskningsinsatser läggs på utvecklingen av alla teknologierna eftersom ingen vet vilken kommer vara vinnaren eller om det kommer krävas en kombination av teknologier. Förutom forskargrupper på universitet och institut har två företag gått in i kapplöpningen, IBM och D-wave.

VAD ÄR D-WAVE? Ett företag som påstår sig ha byggt en storskalig kvantdator. Den är specialdesignad för en viss typ av kombinatoriska optimeringsproblem och har därför inte potentialen att bryta dagens krypteringssystem. Många forskare är skeptiska till företagets påståenden och data som publicerats pekar främst på att D-wave beter sig mest som en vanlig specialiserad dator och inte som en kvantdator. Trots detta har stora företag (Google, NASA, Lockheed Martin) investerat i D-wave men detta kan vara för att testa tekniken och för att studera en ny datorarkitektur.

1.2 Grundläggande kvantmekanik

I vår digitaliserade värld har troligtvis ingen undgått ”biten” vilket är förkortningen av engelskans binary digit. Denna är den minsta representationen av ett tal eller logisk enhet och myntades för första gången 1948 av Claude E. Shannon som oftast anses vara fadern till informationsteorin [4]. Bitens informationsinnehåll representeras ofta av talen 0 och 1. Däremot i alla implementationer, som exempelvis i en datorkrets, representeras biten av ett fysikaliskt system. Detta kan vara allt från hög- eller lågström i en krets, tänd och släckt lampa i morsealfabetet eller korta laserpulser i fiberlänkar.

1.2.1 Kvantbiten

Som nämndes tidigare i introduktionen började fysiker i mitten av 1900-talet att laborera med idén om vad som skulle hända då kretsar krymptes så pass att den klassiska fysiken inte längre är tillämplig och kvantmekanikens lagar tar över. I detta skede generaliserades den klassiska biten till kvantbiten, även kallad på engelska qubit. Likt biten representeras kvantbiten av två tillstånd men dessa motsvarar ett kvantmekaniskt system med två tillstånd vilka representeras av *tillståndsvektorerna* $|0\rangle$ och $|1\rangle$. Till skillnad från en klassisk bit som bara kan anta värdena 0 och 1 kan kvantbiten befinna sig i en superposition av sina kvanttillstånd $|0\rangle$ och $|1\rangle$.

Kvantbitens superposition ger en mycket rikare struktur jämfört med ett klassiskt system. I fallet för biten finns det bara en sak att mäta nämligen om biten är 0 eller 1. Kvantbiten däremot kan mätas på flera olika sätt och kan befinna sig i tillstånd i mellan 0 och 1. Hade tillståndet varit representerat av jorden skulle biten endast befinna sig antingen på nord eller sydpolen, medan kvantbiten kan

befinna sig var som helst på jordytan och på så sett representera information på ett annat sätt än biten. Trots den rikare strukturen, där tillsynes en obegränsad mängd klassisk information kan lagras i kvantbiten, kan bara en bit av information läsas ut då en mätning sker. Det vill säga likt den klassiska biten har kvantbiten bara två utfall men den kan mätas och prepareras på många olika sätt.

1.2.2 Från en till flera kvantbitar

För att bygga kombinerade tillstånd som representerar olika faser i en beräkning behövs flera kvantbitar. Två kvantbitar kan till exempel prepareras på fyra olika bastillstånd 00, 01, 10, 11 men den stora skillnaden mellan klassisk fysik och kvantfysik är att två kvantbitar även kan vara i en superposition av alla fyra bastillstånden samtidigt. Detta är något som är i skarp kontrast till vad som är möjligt med klassiska datorer och skapar en slags parallellism där flera spår i en beräkning kan följas samtidigt.

Antalet termer ökar exponentiellt med antalet kvantbitar, för att vara mer exakt kommer antalet termer att öka med 2^n där n är antalet kvantbitar som är tillgängliga. Denna exponentiella ökning i superponerade termer är en av kvantinformatikens stora styrkor. Bara med 400 kvantbitar initialiserade på korrekt vis kommer superpositionen att beskrivas av ett tillstånd med fler tillståndsvektorer (2^{400}) än antalet fundamentala partiklar i hela universum [5].

Trots denna rika struktur så är inte alla termerna tillgängliga då en mätning utförs eftersom bara ett svar per kvantbit är möjligt. Vid en mätning på n kvantbitar kan 2^n alternativ testas men bara n svar fås. Eftersom endast en glimt av den rika strukturen återspeglas vid en mätning kommer majoriteten av protokollen och beräkningarna vara baserad på att de ska utföras många gånger. Detta för att få ett statistiskt underlag över hur de 2^n olika möjligheterna är fördelade. Denna statistiska insamling är ytterligare en stor skillnad som inte återfinns i beräkningar med klassiska bitar.

1.2.3 Kvantmekanisk snärjelse

Kvantmekanisk snärjelse innebär att två eller fler partiklar är kvantmekaniskt korrelerade till den grad att det inte går att betrakta partiklarna som separata ting. Med snärjelse[f], entanglement på engelska, kan korrelationer skapas som är kraftigare än vad som är möjligt med klassiska korrelationer. Till exempel om två kvantbitar sätts i en superposition av tillstånden 01 och 10 kommer ett snärjt kvanttillstånd att ha skapats. Detta innebär att två partiklar som blivit snärjda och sedan separerats från varandra kan bete sig som om de påverkar varandra trots att

[f] Andra vanligt förekommande formuleringar är: sammanflätning, kvanttrassel, hoptrasslade, inflätade. Vi adopterar här snärjelse efter rekommendation av forskare i ämnet.

de inte är i närheten av varandra när de mäts. Under kvantmekanikens barndom argumenterade Einstein, med andra, emot kvantmekaniken genom att belysa de egendomliga egenskaperna som snärjelse medförde [6]. I ett brev[g] till Max Born beskrev Einstein denna egendomliga egenskap som ”Spooky action at a distance”. Idag anses snärjelse vara en informations och kommunikations resurs som möjliggör spektakulära protokoll som kvantmekanisk teleportering som är en viktig komponent både för kvantkryptering och kvantdatorn.

1.2.4 Mätningar och icke-kloningsteoremet

Med klassisk information är vi vana vid att kunna kopiera eller duplicera informationen. I kvantmekanikens värld är detta inte alls lika enkelt. Under kvantinformationsstudier får studenter lära sig att kvantfysiken inrättar en rad ”negativa” regler som anger saker som inte kan göras. Två exempel är

- Man kan inte utföra en mätning på ett kvantmekaniskt system utan att störa systemet.
- Man kan inte utföra en perfekt kopiering av ett okänt kvantmekaniskt tillstånd.

Dessa två punkter har stora konsekvenser för vilken information som kan tas ut ur ett kvantmekaniskt system och hur omgivningen påverkar systemet. Den första punkten innebär att allt som kopplar till kvantsystemet kan potentiellt störa förloppet och förstöra kvanttillståndet (dekoherens[h] är den tekniska termen för förloppet) och därmed förloras informationen. På grund av detta är det viktigt att kvantsystemet som används är väl isolerad från sin omgivning under den tid som beräkningsförloppet eller transmissionen av kvanttillståndet utförs. Samtidigt ska systemet vara kraftigt kopplad till sitt utläsningssystem när mätningen av kvantbitarna ska utföras. Dessa två aspekter kan låta motsägelsefulla men en del av arbetet är att hitta vägar runt denna problematik.

Den andra punkten kan ses som ett dilemma som uppkommer då en mätning ska utföras. Om endas en partikel med ett okänt kvanttillstånd är tillgänglig skulle det vara fördelaktigt att kopiera upp flera exemplar för att sedan utföra mätningar på var och en av dessa. På detta sätt skulle en full kartläggning av tillståndet kunna göras utan att skicka mer än en partikel. Detta är dessvärre inte möjligt utan att införa brus i systemet. Regeln ger ytterligare en restriktion på informationen som kan tas ut ur ett kvantmekaniskt tillstånd.

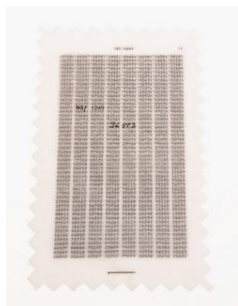
[g] Breven finns att läsa på: https://archive.org/details/TheBornEinsteinLetters
[h] http://www.ne.se/dekoherens

För en djupare introduktion till kvantmekaniken hänvisar vi till den breda floran av böcker som finns tillgänglig, till exempel [7]. I följande avsnitt kommer vi att bekanta oss mer med hur ovanstående principer och andra kan utnyttjas för säker nyckelöverföring och skapandet av kvantdatorn. Dessutom ska vi bekanta oss med de teknologiska begränsningarna och kommersiella system som finns.

2 Kvantkryptografi

Att låsa ett meddelande så att ingen obehörig kommer åt informationen är en mångtusenårig konst. Grundstegen för utförandet är att följa en krypteringsalgoritm, även kallat chiffer, där meddelandet tillsammans med extrainformation, krypteringsnyckeln, kombineras för att få ett kryptogram. Informationen i kryptogramet är bara säkert om chiffret endast tillåter återskapandet av meddelandet genom nyckeln. Detta antagande försvagas oftast i praktiskt användbara sammanhang på grund av tekniska svårigheter och användarbarhet. Istället sätts kravet att det ska vara väldigt svårt att återskapa klartexten utan nyckeln. Termen ”väldigt svår” i kryptografiska sammanhang refererar till komplexitet inom beräkningsvetenskap där innebörden är att tiden det tar att utföra uppgiften ska växa exponentiellt med antalet bitar i kryptogramet. Detta jämfört med en polynomiell tid som klassificerar ”enkla” problem, se faktaruta om polynomiell och exponentiell tid.

Exempelvis är säkerheten i dagens populära RSA-kryptering (skapat 1977 och fick namnet efter upphovsmakarna Ron Rivest, Adi Shamir, Len Adleman) baserad på faktorisering av stora tal som är klassificerat som svårt med dagens teknik. Motsatsen, multiplikation, som används för att skapa kryptogramet är desto enklare att utföra eftersom det bara behövs göras en gång. Just i fallet RSA-kryptering har säkerhetsantagandet visat sig vara hotat då effektiva kvantalgoritmer för faktorisering har hittats, vilket vi återkommer till längre fram.



En krypteringsmetod som visat sig vara omöjlig att knäcka, om den används på korrekt vis, är engångskryptot. Styrkan med detta chiffer är att kryptogramet kommer att vara fullständigt slumpartat och endast den korrekta nyckeln kommer att återskapa klartexten. Nackdelen med chiffret är att parterna, som här benämns Alice och Bob, måste i förhand ha delat nyckeln sinsemellan. Dessutom kan nyckeln bara användas en enda gång och därav namnet. Principen som används är att Alice och Bob har sinsemellan identiska sekvenser av slumptal. Då Alice ska skicka ett meddelande till Bob tas en lika lång sekvens av slumptal som meddelandet och en enkel operation utförs för att addera meddelandet med slumptalssekvensen. Kryptogrammet som fås har matematiskt bevisats vare fullständigt säkert oavsett datorkraften som används. För att återfå klartexten tar Bob fram sin nyckel, som är identisk till Alice, och utför en subtraktionsoperation. Hela chiffret är så enkelt att endast penna och papper behövs för att kryptera ett meddelande. Chiffret har används under 1900-talet då mycket delikat information måste hemlighållas. Miniatyrböcker och

frimärken, se bilden[i] ovan, med slumptal delades ut mellan parterna så att de lätt kunde gömmas undan.

Trots sin enkelhet har engångskryptot många problem som gör den opraktisk för användning i stor skala. Dess säkerhet ligger i att först kunna generera riktiga slumpsekvenser för krypteringsnyckeln. Bara detta är en konst för sig för dagens slumpgeneratorer, som sitter i bland annat datorer, har visat sig inte generera helt slumpvisa serier. Sedan måste slumpsekvensen distribueras mellan Alice och Bob på ett säkert sätt. Slutligen kan varje sekvens bara användas engång. De sistnämnda gör att nya nycklar måste distribueras kontinuerligt för att engångskryptot ska bli praktiskt användbart. Det är här i distributionsprocessen av krypteringsnyckeln som kvantmekaniken hjälper till. Kvantkryptografi är således inte ett chiffer för att koda information utan en säker distributionsmetod av slumptal, dvs. krypteringsnycklar, som sedan kan användas i ett engångskrypto. Kvantmekaniken har mekanismer för slumptalsgenerering som tillsammans med kopieringsrestrektionerna gör den till en kandidat för distribueringen av krypteringsnycklar.

***Faktaruta om polynomiell och exponentiell tid*:** Inom datavetenskap klassificeraras beräkningsproblem enligt hur väl algoritmen för att lösa ett problem presterar. Ofta pratar man om hur tiden det tar att lösa problemet skalar då storleken på problemet ökas. Två kategorier som återkommer är lösningar där tiden ökar polynomiellt (**P**) eller icke-polynomiellt där exponentiell tillhör de senare. Dessa två klasser kan beskrivas som problem där en lösning kan fås på rimligtid även om problem storleken ökas respektive problem där en ökning i problemstorleken medför en så stor tidsökning att stora problem blir i princip omöjliga att utföra. Man kan säga att det existerar lika-med tecken mellan polynom och ”effektiv”, ”snabb” osv.

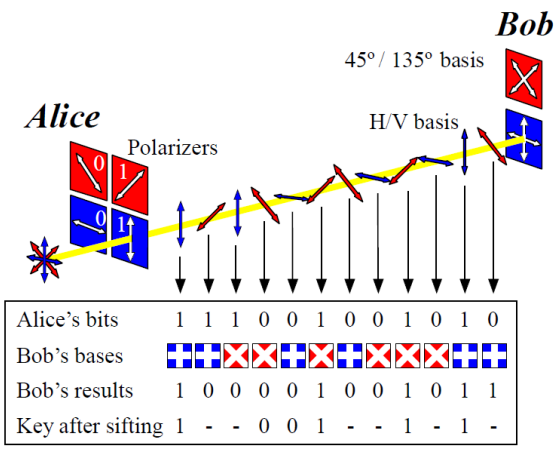
Ett exempel på ett problem som skalar exponentiellt är primtals-faktorisering. Detta betyder att med dagens klassiska algoritmer ökar tiden mycket fort då primtalsfaktorerna ska hittas på allt större tal. Talet 15 kan beskrivas med 3 bitar gentemot talet 10580873 som behöver 23 bitar för att skrivas i binärform. Båda dessa tar bara någon tusendels sekund att faktorisera med dagens datorer, $3 \cdot 5$ respektive $3571 \cdot 2963$. Ökas problemet till tal som beskrivs med 300 bitar ökar faktoriseringstiden till timmar, 600 bitar tar flera år och tal med 1000 bitar tar miljontals år. NIST rekommenderade RSA nyckel längd är på 2048 bitar.

[i] Bilden är från: www.flikr.com ”One-time pad” www.usa.gov/copyright.shtml

2.1 BB84

Ett av de mest kända kvantnyckelöverföringsscheman BB84, och de tidigaste, utformades 1984 av Charles H. Bennet, då på IBM, och Gilles Brassard från Montréals universitet. De fann att kvantmekanikens ”negativa” restriktioner, som vi introducerade ovan, kan vändas till att öka säkerheten. Bennet och Brassard insikt baserade sig på att under transmissionen av ett kvantmekaniskt system mellan två parter så kommer alla försök att avlyssna alltid att introducera brus. Logiken är att om inget brus återfinns mellan parterna, Alice och Bob, då kan inte kvantsystemet som skickats över blivit manipulerat av en illasinnad Eve (från engelskans eavesdropper), alltså har informationen på ett säkert sätt överförts. Det speciella med insikten var att naturlagar ger informationsrestriktionen och därmed säkerheten. Detta kan jämföras med klassiska system som baseras på teknologi där säkerheten uppkommer av svårigheten att lösa ett problem, exempelvis RSA-krypteringsprotokollet där säkerheten förlitar sig på svårigheten att faktorisera stora tal.

En populär angreppspunkt för att beskriva själva kvantnyckelöverföringsschemat baserar sig på fotonens polarisationsegenskaper. Principen illustreras i Figur 1. Alice väljer slumpvis mellan fyra olika polarisationstillstånd att polarisera fotonen i, vilken sedan skickas till Bob. På Bobs sida väljs mellan de två polarisationsbaserna slumpvis för att mäta fotonen. Eftersom Bob inte vet vilken bas Alice skickar i kommer endast 50% av valen att resultera i korrekta resultat.



Figur 1: Illustration av BB84 protokollet [8]. Alice väljer slumpvis mellan sina fyra polarisationer och registrerar basen och vad som hon skickar (Alice’s bits), Bob väljer mellan sina två mätbaser (Bob’s bases) och registrera resultatet av mätningen (Bob’s results). Efter en publik annonsering av Bob’s bas val kan Alice och Bob sortera bort alla gånger fel bas användes (Key after sifting). Resultaten är en perfekt korrelerad bitsträng mellan Alice och Bob om ingen har försökt att tjuvlyssna.

Vilka resultat som är korrekta fås då Alice och Bob, efter att ha skickat många fotoner, annonserar i en öppen kanal vilken polarisationsbas som används för varje skickad foton (Bob's baser i Figur 1). Observera att Alice och Bob inte avslöjar vilken polarisation som skickades utan bara basen. Nu kan en jämförelse mellan Alice och Bobs publikt annonserade bas val göras och där hitta fotonerna med samma bas. Vetskapen om att samma bas val har används i sändningen och mätningen kommer att resultera i korrelerade svar mellan Alice och Bobs resultat av polarisationstillståndet av fotonen (svarsremsan längst ner i Figur 1). Till exempel då Alice skickar diagonal polarisation och Bob mäter i basen diagonal/antidiagonal-polarisering kommer båda att få att fotonen var diagonalt polariserad vilket är inkodningen på 0. Hade Alice istället skickat antidiagonal-polarisering skulle Bob också få antidiagonal vilket är kodat till 1. På så sätt får varje korrekt bas val mellan Alice och Bob en associerad 0 eller 1.

En tjuvlyssnande Eve kommer på grund av kvantmekanikens regler alltid införa extra brus. Detta kommer att yttra sig genom att, i de fall då Alice och Bob valt samma bas, polarisationsmätningen mellan parterna inte längre är perfekt korrelerade. Ett bruspåslag kommer att finnas och så sätt avslöja att överföringen har blivit uppfångad av en tredje part. Genom att slumpvis jämföra vissa delar av den slutgiltiga strängen, via an publikkanal, kan brusnivån uppskattas. Om nivån på bruset är under vissa tröskelvärden kan nyckelsäkerheten garanteras. Den resterande nyckeln kan nu i princip användas för att utföra ett engångskrypto [9], [10], [8].

2.2 E91

BB84's enkelhet och elegans baserar sig på att Alice distribuerar kvantbitar till Bob. Detta låser protokollet till endast två parter. En version där distributionen kan ske från en tredje part baserar sig på snärjda tillstånd. Artur Ekert föreslog 1991 att istället för att låta Alice slumpvis skapa fotoner med olika polarisationstillstånd som sedan skickas till Bob kan kvantmekaniken åta sig slumpgenereringsrollen. Genom att distribuera ett snärjt kvanttillstånd mellan Alice och Bob kan ett likvärdigt protokoll till BB84 utföras men med några fördelar.

Fördelarna är att först behöver distributionen inte längre vara låst till Alice eller Bob utan kan vara placerad på en annan plats. Detta möjliggör att inte bara Alice och Bob kan ta del av partiklarna. Med relästationer i fibernätverk kan distributionen av fotonerna ske till andra parter som skulle behöva kommunicera på ett säkert sätt. Den andra fördelen ligger i att snärjda tillstånd inte kan beskrivas med klassiska korrelationer. För att ta reda på om Eve tjuvlyssnat kan parterna utföra ett så kallat Bell-test. Testet är utformat som en matematisk olikhet som beskriver gränsen för hur högt värde en korrelation kan uppnå med hjälp av endast distribuerade klassiska medel. Genom att visa att det

distribuerade kvantmekaniska systemet bryter olikheten kan säkerheten i nyckeln garanteras.

Planer för att skicka upp satelliter[j] som ska distribuera snärjda fotoner över stora avstånd finns både i Kanada [11], Europa [12] och Kina [13]. Som ett första steg har Österrike med en serie experiment visat att långdistansdistribution av fotoner via teleskop mellan Teneriffa och La Palma (143 km) är genomförbart. Experimentet hade en nyckelöverföringshastighet på endast 13 bit/s men högre överföringshastigheter förväntas med bättre metoder för att skapa snärjda fotoner.

Den mest effektiva metoden för att skapa par av snärjda fotoner är idag via en icke-linjär optisk process som kallas SPDC (Spontaneous Parametric Down Conversion). I processen används en stark laser som fokuseras på en icke-linjär kristall. Med en låg sannolikhet kan en laserfoton dela sig och bli två där båda har lägre energi än ursprungsfotonen. När allt är korrekt konfigurerat kan snärjelse i polarisationen skapas mellan fotonerna som emitteras ut ur kristallen. Sådana fotonkällor finns idag som demonstrationsutrustning på högskolor och mera avancerade varianter används för forskningsändamål. Planerna för en satellitbaserad distribution av snärjda fotoner inkluderar kompakta och effektiva SPDC fotonkällor.

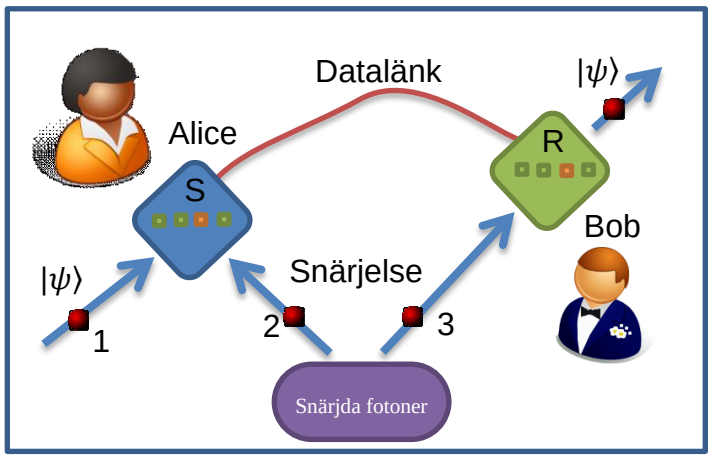
2.3 Kvantmekanisk teleportering

En effekt som är relaterad till kvantkryptografi men som även är mycket viktig i kvantdatorsammanhang är kvantmekanisk teleportering. Detta ska inte förväxlas med science fiction termen där materia försvinner från ett ställe och återmaterialiseras på ett annat. Kvantversionen av teleportering är inte desto mindre spektakulär men har sina fysikaliska begränsningar. Det som teleporteras är kvanttillståndet och inte partikeln i sig, dessutom förstörs informationen i originalet för att inte strida mot icke-kloningsteoremet. I de enklaste protokollen fungerar det så att först distribueras ett snärjt kvanttillstånd mellan två parter. Detta kan göras via satellit eller genom fibernätverk. Dessa distribuerade partiklar antas kunna förvaras för senare bruk utan att förstöra det snärjda tillståndet som råder mellan de två separerade partiklarna. När ett kvanttillstånd ska teleporteras utförs en speciell typ av mätning mellan en snärjd partikel och kvanttillståndet som ska överföras.

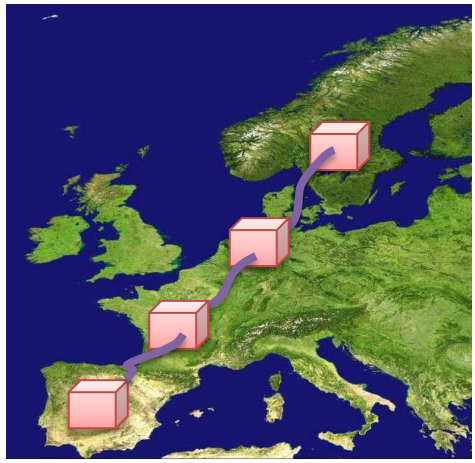
Vad som är viktigt att notera är att även om kvantteleportering av själva informationen om tillståndet kan ske omedelbart blir inte den tillgänglig förrän informationen om vad tillståndet innebär också blivit överfört. Detta måste göras på traditionellt vis eftersom detta motsvarar en liten mängd klassisk information

[j] Se ett föredrag om satellitbaserad kvantnyckel överföring: Satellite-based quantum communications – Jane E Nordholt: www.youtube.com/watch?v=x41N6vVcB48

från en mätning. Detta innebär att hastigheten på överföringen av *information* begränsas av klassiskt överföring vilket gör att man fortfarande begränsas av ljusets hastighet precis som idag. Teleporteringsprotokoll har demonstrerat mellan öarna Teneriffa och La Palma [14].



Figur 2: Illustration av teleporteringsprotokollet. Alice teleporterar över tillståndet 1 till Bob genom att utföra en mätning mellan partikel 1 och partikel 2 där den senare är snärjd med partikel 3. Efter Alice mätning **S** får hon ett av fyra svar som måste skickas till Bob via datalänken för att fullborda teleporteringen genom att applicera en av de fyra transformationerna **R**.



Figur 3: Illustration[k] av hur ett nätverk av ”kvantupprepare” (quantum repeters) kan användas för att brygga stora avstånd då ett kvanttillstånd ska överföras [15].

Kvantteleportering är en viktig komponent i distributionsledet av kvanttillstånd. När ett en-fotonstillstånd ska transporteras mellan två punkter via fiber eller trådlöst med teleskop är avståndet begränsat på grund av förluster. En metod som är under utveckling är att använda teleportering i sekvenser och låta kvanttillståndet hoppa fram med hjälp av ”kvantupprepare” (quantum repeters), se Figur 3. Detta skulle kunna brygga avståndsproblemet som alltid finns vid direkt överföring vilket har en övre gräns på ett par hundra kilometer. Kommersiella system har visat räckvidder på under 100km och laboratoriesystem har nått upp till 250km men alla med mycket varierande överföringsförmåga från hundratals bit per sekund till kilo eller mega bit per sekund för kortare avstånd. Överföringshastigheten är mycket beroende av fiberlängden vilket ger en praktisk övre gräns på ungefär 150km.

[k] Kartbilden är från: Wiki Commons

2.4 Kvantmekanisk hemlighetsdelning

I vissa scenarier är det önskvärt att dela en hemlighet mellan flera parter där ingen av parterna för sig ska kunna ta del av hemligheten. Detta skulle kunna vara delningen av en kassaskåpsnyckel mellan flera anställda där de måste sammarbeta för att öppna kassaskåpet. Denna problemställning har generaliserats till en kvantmekanisk version där hemligheten är ett kvantmekaniskt tillstånd. Tillståndet kan användas för att dels dela en krypteringsnyckel men också annan information kan delas med hjälp av kvanttillståndet. Många olika typer av protokoll har föreslagits, varje med sina fördelar och kodningsmöjligheter.

2.5 Teknologier inom kvantkryptografin

Vi har i tidigare delkapitel gett en överblick av de grundläggande principerna som ligger till grund för forskningsfältet kvantkryptering. Forskningsfältet drivs dels av att hitta nya teoretiska metoder för att distribuera och bevara hemligheter men också att hitta metoder att praktiskt demonstrera dessa förmågor. Stora delar av fältet ligger än idag i grundforskningsstadiet där det är framförallt proof-of-concept experiment som utförs, men detta är på väg att ändra sig. Protokoll som inte är baserad på snärjelse har nu kommersialiserats av flera företag från bland annat Schweiz, Österike, Frankrike och USA.

2.5.1 Kommersiella aktörer

De kommersiella produkterna inom kvantkryptografi baseras uteslutande på en-fotonsprotokoll med en direkt länk mellan parterna. Dessa är alla grundade i BB84 protokollet med vissa modifikationer för att öka säkerheten och räckvidden. Dvs. kvantkrypteringen är baserad på att informationen är kodad i en enda foton t.ex. genom polarisation. I bästa fall ska en en-fotonkälla användas, men kostnad och utbud har drivit fram kvantkrypteringsprotokoll som baserar sig på lasrar där ljuseffekten har reducerats kraftigt för att skapa en approximativ en-fotonkälla. Detta gör systemet sårbart eftersom flera fotoner kan emitteras samtidigt av lasern. Genom att variera intensiteten på lasern kan implementering av ”bulvan–tillstånd” (decoy states) utföras vilket återställer säkerheten. Även räckvidden på fiberlänken kan förlängas genom denna metod. Företagen är indelade i två läger där Idquantique och MagiQ använder en teknologi där fotoner detekteras och räknas via en direkt mätning medan Sequrenet och Quintessencelabs använder en detektionsmetod där en stark laserstråle, som fungerar som en förstärkare, blandas med en-fotontillståndet, som bär nyckeln, för att finna och detektera fasen med en klassisk pin-diod.
Flera företag har börjat intressera sig för kvantkryptering och enklare kvantprotokoll som möjliggör exempelvis slumptalsgenerering och säker nyckelöverföring. Några av aktörerna är:

Idquantique[l]**,** erbjuder fiberoptiskt baserade kvantnyckelöverföringssystem där flera lager av klassisk- och kvant-kryptering används för att garantera säkerheten med en räckvidd upptill 100km. Förutom krypteringssystem erbjuds produkter för slumptalsgenerering via kvantmekaniska principer med mycket höga utläsningshastigheter. Alla systemen bygger på teknologi där sekvenser av enstaka foton transmiteras och detekteras. Företaget var den första kommersiella aktören och demonstrerade kvantkrypteringsystemet under det Schweiziska valet 2007. De driver även projektet Swissquantum som demonstrera ett nätverk för kvantkryptering mellan flera Schweiziska städer.

MagiQ[m], säljer kvantkrypteringsystem baserad på en-foton-teknologi med upp till 50km räckvidd.

Quintessencelabs[n]**,** erbjuder ett system baserad på kontinuerlig laserstrålning. Partner med Lockheed Martin och support från Telstra.

Sequrenet[o]**,** franskt företag som erbjuder kvantkryptering via kontinuerlig laserstrålning. Räckvidden upptill 80km med 100bit/s och vid 20km 10kbit/s.

Toshiba[p], utvecklar kvantkrypteringssystem och dess komponenter. T.ex. utvecklas kvantprickar som kan emittera enskilda fotoner.

2.5.2 Protokoll för snärjda fotoner

E91 protokollet som diskuterades tidigare är grunden till flera andra där ett är kvantteleportering. Men på grund av svårigheterna att skapa snärjda fotoner har inga kommersiella aktörer anammat protokollet och är därför endast demonstrerat i forskargrupper. Andra intressanta protokoll har på senare tid visat att med snärjda kvantbitar kan säkerhet bortom kvantmekaniken garanteras. Alla datorer och kommunikationssystem är implementerade i ett fysiskt system. Vi bygger säkerhet genom att analysera hur dessa system kan manipuleras enligt fysikens lagar. Om vi har fel om vilka fysikens lagar är blir analysen fel och säkerheten hotas. Säkerhet bortom kvantmekaniken handlar om att göra så få antaganden som möjligt i säkerhetsanalysen så att säkerheten blir robust även om fysikerna har fel beträffande fysikens lagar. Vissa av dessa nya protokoll har även visats ha möjligheten att kunna minska antaganden om utrustningen som används. Innebörden är att i vissa fall spelar det inte längre någon roll vem som har byggt utrustningen. Protokollet tillsammans med snärjelsen ser till att en tjuvlyssnare som försöker manipulera utrustningen inte kan få tillgång till informationen utan att röja sig [16], [17]. Dessa protokoll är idag endast

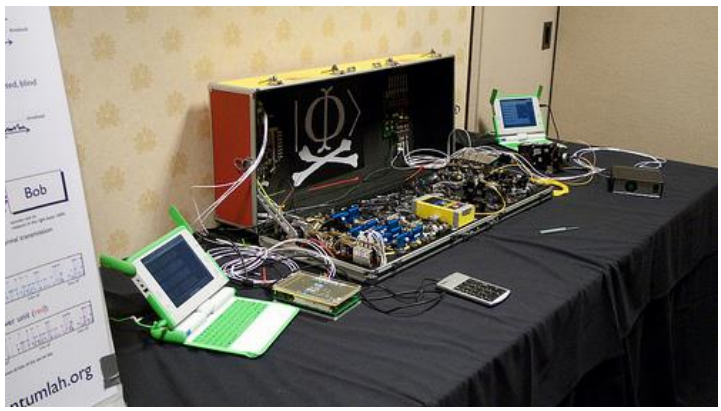
[l] Hemsida: idquantique.com/
[m] Hemsida: magiqtech.com/Home.html
[n] Hemsida: quintessencelabs.com
[o] Hemsida: www.sequrenet.com
[p] Hemsida: www.toshiba-europe.com/research/crl/qig/quantumkeyserver.html

teoretiska men forskning görs för att se hur mycket som kan implementeras experimentellt. Det är tvivelaktigt om dessa förslag kommer att kunna implementeras till fullo men varje litet steg kan förstärka säkerheten.

2.5.3 Hur säkra är kvantkrypteringsimplementeringar

Kvantkrypteringsteorin har ett elegant och generellt bevis för att garantera säkerheten med hjälp av fysikens lagar. Men i en implementation kommer de teoretiska antagandena och abstrakta principerna inte kunna följas fullt ut. Trots de teoretiska framstegen att avlägsna teknikberoendet i kvantkryptering är det troligt att det alltid kommer finnas bakdörrar där en infiltratör kan utnyttja systemets svaga punkter [9].

Som en motoffensiv för att granska de kommersiella och experimentella systemen har Vadim Makarov[q] utfört flera attacker mot kvantkrypteringsystem. Detta för att visa att mognadsgraden inte riktigt är uppnådd och att förvarna utvecklarna om brister så att de kan implementera motmedel. Med hjälp av starka laserpulser har Makarov visat att krypteringssystem som inte skyddar sina detektorer kan tas över. I värsta fall kan Eve ha fullkontroll över Alice och Bobs utrustning, se Figur 4.



Figur 4: Vadim Makarovs utrustning för att hacka kvantkrypteringssystem[r].

Han visade även 2008 att Idquantiques system hade problem i slumptalsgenereringen av Alice val av baser vilket ledde till att vissa mönster fanns i de utsända kvantbitarna. Företaget kontaktades och buggen togs bort. För

[q] Alla hans artiklar kan hittas under publications på: www.vad1.com

[r] Bild från: www.flickr.com/photos/aramosorg/4169604320
creativecommons.org/licenses/by-nc-sa/2.0/

en överblick av olika svagheter och kvantkryptering protokoll se Vadim Makarovs föreläsning från IQC[s] i Kanada.

Säkerheten för systemen baserade på homodynmätningar har inte i samma utsträckning blivit attackerade men det är förväntat att dessa har minst lika många bakdörrar. Redan i protokollet är det osäkert om dessa är säkra eftersom den starka lasern, som fungerar som en förstärkare, måste skickas mellan Alice och Bob.

[s] IQC (Information for quantum computing) föreläsning: www.youtube.com/watch?v=5kUARd_y53w

3 Kvantdatorn

En internet-sökning på termen ”kvantdator” ger uppfattningen av att den är redan här. Både Google, NASA och Lockheed Martin påstås ha en kvantdator från D-wave systems samtidigt som IBM är på god väg att utveckla sin version av kvantdatorn. Stora rubriker skrivs i både teknikorienterade tidningar och i dagspressen men hur ser situationen ut om vi gräver lite i ämnet. Hur väl fungerar D-wave? Och hur långt har teknologiutvecklingen kommit?

Den tillgängliga mediala informationen kring kvantdatorn kan ofta kännas spretig, till viss del mystisk och med avsaknad av djupare motiveringar och tillhörande kritik. Detta är troligtvis på grund av att ämnet kräver relativt djupa förkunskaper och att det inte finns en entydig teknikinriktning som gå att bevaka. Vitt skilda forskningsområden som arbetar med kvantmekanik har potential att bli huvudkandidater eller vara viktiga för specifika problemställningar.

Låt oss börja med att introducera och diskutera vad en kvantdator är, dess förmåga och förväntade användningsområden. Sedan tar vi och fördjupar oss i några olika beräkningsmodeller och kvantdatorarkitekturer med möjliga implementationer.

3.1 Vad är en kvantdator och vad är den inte

Kvantdatorn ses ofta som en separat entitet som kommer att ersätta den klassiska datorn. Vi tror att denna utveckling inte är trolig, istället förutses ett hybridsystem där kvantdatorkapacitet ges via en hjälpprocessor till de klassiska systemen [18]. Utvecklingslinjen för det kvantmekaniska hjälpsystemet kommer att vara högspecialiserat till en början. Hårdvaran kommer att vara dedikerad till specifika kvantalgoritmer. Två exempel skulle kunna vara den berömda faktoriseringsalgoritmen som Peter Shor presenterade 1994 [19] eller experiment som simulerar en viss typ av kvanteffekter [20] i ett mera kontrollerbart kvantsystem än de faktiska.

Mycket av det mediala intresset för kvantdatorn har just kretsat kring Shors upptäckt på grund av att den ger möjligheten till att bryta dagens RSA-kryptering vars säkerhet bygger på att det är svårt att faktorisera stora tal med klassiska datorer. Trots att detta är en applikation med samhällsomvälvande konsekvenser så fokuserar forskarvärlden mera på bredare frågeställningar som t.ex. de simuleringsmöjligheter som förväntas komma med kvantdatorn. Redan idag finns specialiserade experimentella system som inriktar sig på specifika simuleringar och problemställningar. Exempelvis strävar företaget D-wave mot utvecklingen av kvantdatorer specialiserade på en viss typ av kombinatoriska optimeringsproblem. Andra exempel är simuleringar av magnetiska egenskaper för supraledande material via fria atomer som hålls fångade i ett gitter skapat av

laserljus [20]. Sådana simuleringar antas kunna ge nya insikter i studier av högtemperatursupraledning som skulle kunna minska energiförluster i elnät och spinntronik som är en kandidat till kvantdatorn, men används även inom medicinsk avbildning. Shors faktoriseringsalgoritm har demonstrerats för talen[t] 15 och 21 med olika specialiserade experimentella uppställningar, dels med kärnmagnetisk resonans [21] och dels med fotoner [22]. Många av experimenten är mer proof-of-concept och har inte bidragit med ny kunskap genom simuleringen men allt fler experiment har kunnat inrikta sig på icke-triviala simuleringar som den med atomer i ett ljusgitter.

I dagsläget är det mycket svårt att uttala sig om beräkningskapaciteten och beräkningstiden för ett praktiskt utförande av en kvantalgoritm med ett stort antal kvantbitar. Detta mest på grund av att kapaciteten är hårt kopplad till implementationen av kvantdatorn. Här finns många olika teknologiska möjligheter som visats fungera för enstaka kvantbitar men än har ingen skalning av systemen demonstrerats. En analys av svårigheterna ges av [18] där de har extrapolerat tiden det tar att utföra Shors algoritm med några olika teknologier och nuvarande experimentella parametrar. I analysen har författarna jämfört NIST rekommenderade RSA nyckellängd och prestandan på NFS (Number Feild Sieve), som är en klassisk faktoriseringsalgoritm, med olika kvantdatorteknologier. Slutsatsen de drar är att "fel" kvantdatorteknologi inte ger några fördelar gentemot NFS trots den icke exponentiella tidsutvecklingen som kvantalgoritmen ger. Men med ”rätt” teknologi kommer NIST nyckel-rekommendation kunna brytas inom en dag!

3.1.1 Hur skiljer sig en kvantdator från en vanlig dator

En klassisk dator utför beräkningar genom att manipulera bitar. De grundläggande operationer som behöver kunna utföras på en bit är OCH och INTE. INTE-operationen omvandlar 0 till 1 och 1 till 0. OCH-operationen tar två bitar som indata och ger 1 i resultat om båda indata-bitarna har värdet 1, annars 0. Allting som kan göras med en klassisk dator kan uttryckas som en följd av OCH- och INTE-operationer. Kvantbitar, som förklaras i sektion 1.2, är försöket att generalisera biten med hjälp av kvantfysik. Förutom kvantbiten behövs också operationer som manipulerar kvantbitar.

Programmering av klassiska datorer görs inte på bitnivå. Ett steg upp i abstraktionsnivå finns det som kallas för maskinkod (eller assembler), där programmeraren har tillgång till register och minne och har en uppsättning instruktioner som t.ex. ”Addera två tal”, ”Hoppa till den här adressen om

[t] Det finns fall av faktorisering som är extra lätta. Ett exempel är att faktorisera talet $N = p \cdot q$ om p, q har formen $2^s + 1$. Därför är demo av faktorisering av $15 = (2^1 + 1) \cdot (2^2 + 1)$ inte så imponerande.

registret är 0”. Instruktionerna lagras i datorns minne och processorn utför dem en efter en. De flesta program skrivs i högnivåspråk, som liknar naturligt språk men har en entydig tolkning. Högnivåspråken översätts till maskinkod med en kompilator eller interpretator.

För kvantdatorer krävs också programmeringsmetoder. De algoritmer som finns idag formuleras oftast i termer av enkla manipulationer av kvantbitar som liknar OCH- och INTE-operationerna. Det finns dock en del ansatser att definiera högnivåspråk för att beskriva även kvantdatorberäkningar[u].

Inom matematikområdet beräkningsteori studeras vilka beräkningar som går att få svar på i olika beräkningsmodeller. Området är för stort för att gå in på i detalj här. Den vanligast förekommande beräkningsmodellen är Turingmaskinen, som också är en enkel representation av en riktig dator. En berömd hypotes, Church-Turing-hypotesen, säger att alla beräkningar som går att utföra kan göras av en Turingmaskin. Två andra vanligt förekommande beräkningsmodeller är lambda-kalkyl och rekursiva funktioner; det går att bevisa att dessa tre är ekvivalenta. Ett exempel på en beräkning som inte går att utföra är att avgöra om ett program kommer att stanna och ge ett resultat eller om det fortsätter att köra i all oändlighet.

Området komplexitetsteori studerar vilka resurser som krävs för att utföra en beräkning. Med utgångspunkt i Church-Turing-hypotesen väljs ofta Turingmaskinen som beräkningsmodell, eftersom den är enkel att resonera kring. De resurser som beskriver Turingmaskinen är hur lång tid det tar att utföra beräkningen och hur mycket minne som den använder under beräkningen.

Inom komplexitetsteori definieras olika komplexitetsklasser och problem placeras i dessa beroende på sina resurskrav. Resurskraven beror på hur stort problemet är. En vanligt förekommande komplexitetsklass är P, som står för ”polynomiellt beräkningsbara” och innefattar alla problem för vilka det går att skriva ett Turingmaskin-program som ger svaret på problemet efter en tidsperiod som mest är ett polynom i problemstorleken, samtidigt som den använder begränsat med minne. Klassen P betraktas ibland som klassen av problem som går att lösa effektivt. Det kanske mest kända olösta problemet inom teoretisk datalogi är frågan om klassen P är densamma som klassen NP (non deterministic polynomial), se faktaruta i kapitel 2. NP kan beskrivas som mängden av alla problem där det går att verifiera att en lösning stämmer på som mest polynomiell tid. En speciell delmängd av NP är NPC (NP Complete), som enkelt kan beskrivas som de mest intressanta problemen i NP. Även för kvantdatorer går det att definiera beräkningsmodeller och komplexitetsklasser, se Figur 5. Church-Turing-hypotesen har utvidgats till den fysikaliska Church-Turing-hypotesen, som säger att alla beräkningar som går att utföra enligt fysikens lagar kan utföras

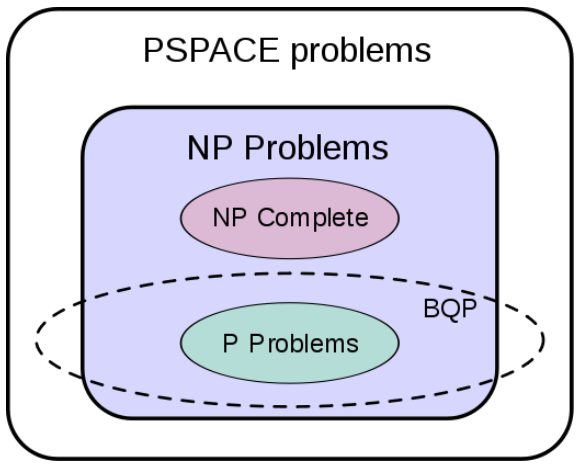
[u] Några försök till programmeringsspråk finns på:
http://en.wikipedia.org/wiki/Quantum_programming

med en Turingmaskin. Förutom utvecklingen och manipulering av kvantbitar och kvantalgoritmer pågår också mycket forskning om kvantkomplexitetsklasser.

Ett vanligt förekommande missförstånd är att kvantdatorer kan lösa alla NPC-problem på polynomiell tid, det vill säga effektivt. Det är dock fortfarande en öppen fråga om så är fallet och det finns en hel del indikationer på att NPC-problem i allmänhet *inte* går att lösa på polynomiell tid på en kvantdator.

En viktig kvantkomplexitetsklass är BQP, som är mängden av alla problem där det går att hitta en lösning vars felsannolikhet är mindre än hälften polynomiell tid på en kvantdator. Eftersom alla kvantberäkningar kommer att vara stokastiska så är detta den mest intressanta kvantkomplexitetsklassen.

Det är inte känt exakt hur BQP förhåller sig till andra klasser, men man tror att det finns problem som finns i BQP men inte i P och att det finns problem som finns i NPC men inte i BQP. Alltså att BQP är ett mellanting mellan P och NPC. Två av de problem som går snabbare att lösa med kvantdator än med en klassisk dator, faktorisering (Shors algoritm) och diskret logaritm är exempel på problem som tros ligga utanför P men inte vara i NPC.



Figur 5:Illustration[v] över hur komplexitetsklasserna är relaterade till varandra och hur man tror att BQP ligger i förhållande till de andra.

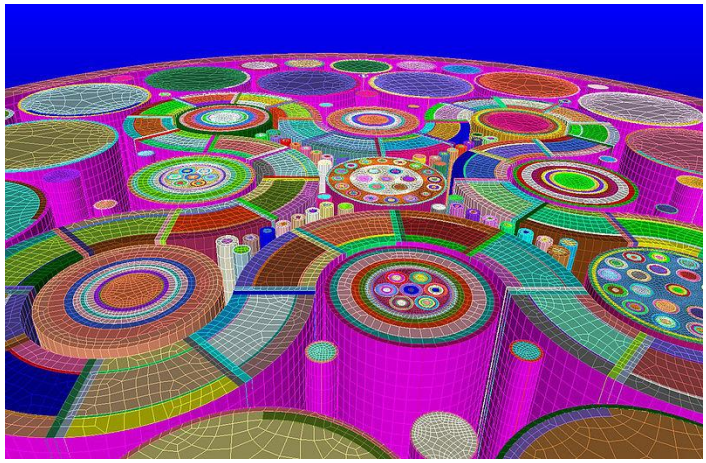
[v] Bild från Wikipedia Commons

3.1.2 Kvantdatorns användningsområden

3.1.2.1 Simulering av fysikaliska system

Ett av problemen som finns med tillverkning av solceller och medicin är att det är väldigt dyrt och tidskrävande att testa alla möjliga konfigurationer av hur atomer, molekyler och andra mer komplexa system som aminosyror kan kopplas ihop för maximal effektivitet. Detta försöker man lösa genom att simulera komponenterna i en dator för att kunna se hur de fungerar innan man tillverkar själva produkten. Eftersom systemen ofta är extremt komplexa räcker oftast inte beräkningskraften till för att ens simulera några tiotal atomer tillfredställande, och med växande antal komponenter växer också komplexiteten exponentiellt. Dessutom är det extremt svårt, och i de flesta fallen omöjligt, att med tillfredställande exakthet simulera ett kvantmekaniskt problem med klassiska metoder [23]. Richard Feynman skissade redan 1982 [1] om hur kvantdatorer skulle kunna simulera kvant-mekaniska system och på så sätt komma runt de här problemen. Kvantsimulatorer kan potentiellt återskapa hur biologiska och kvantmekaniska system beter sig och på så sätt få väldigt exakta och snabba lösningar.

Än kommer det att dröja innan vi ser storskaliga kvantmekaniska simuleringar på en fullskalig kvantdator. Men allt flera experiment inriktar sig på mindre simuleringar av kvantmekaniska effekter. Med bara ett par kvantbitar kan simuleringar som är beräkningstunga för en vanlig dator utföras. Simuleringar som har gjorts är än bara enkla modeller men experimenten blir allt mer sofistikerade [24].



Figur 6: Bild[w] på en simulering av INLs (Idaho National Laboratory) test-reaktor. Här simulerad ända från atomnivå till full-skaliga reaktordelar.

3.1.2.2 Faktorisering av stora heltal och Shors algoritm

Faktorisering av tal innebär att hitta heltals-faktorerna som bygger upp ett givet tal. Som exempel är faktorerna av 143 primtalen 11 och 13 (eftersom $11 \cdot 13 = 143$). När talet blir väldigt stort finns det ingen enkel lösning att hitta faktorerna på och problemet blir väldigt svårt att lösa, speciellt när talet byggs upp av två ungefär lika stora tal. Det här leder till en asymmetri i lösningen eftersom multiplikationen av två primtal, säg 11 och 13 görs med *en* operation, medan faktoriseringen måste göras med många operationer, se faktarutan om *heltals-faktorisering*. Det är den här asymmetrin man utnyttjar i många av dagens chiffer där låset består av att faktoreringen är oerhört tidskrävande, ett exempel på chiffer som är baserad på denna princip är RSA-kryptering vilket används flitigt inom bankväsendet. Med dagens teknik och algoritmer blir klassisk heltals-faktorisering ett oanvändbart sätt att försöka hacka ett kryptogram. Å andra sidan om man har ena faktorn är upplåsningen trivial och därmed lättanvänt.

[w] Från Wikipedia Commons

Faktaruta om naiv heltals-faktorisering: Givet ett heltal *n* kan man hitta dess faktorer genom att iterera ökande heltal med start ifrån 2 och testa division upp till *n* själv. Givetvis behöver man inte gå längre än $\sqrt{n}$ eftersom minst en faktor måste vara mindre än detta. Dessutom har man testat 2 kan man hoppa över alla jämna tal, och har man testat 3 kan man hoppa över alla produkter av tre som 9, 27 osv. På så sätt kan iterationerna reduceras till bara primtal. För att hitta lösningen på *n* = 143 så testas alltså bara primtal mindre än 12 ($\sqrt{143} \approx 12$). Den här lösningen fungerar intuitivt och relativt snabbt på begränsade tal men blir talen stora finns ingen lösning hur man kan göra det inom rimlig tid.

Det finns ingen känd algoritm som kan lösa faktoriseringen med klassiska metoder där tiden för att lösa problemet inte växer exponentiellt med storleken på talet. Det Shors algoritm gör som är unikt för kvantalgoritmen är att lösa uppgiften i polynomiell tid genom att utnyttja superpositions egenskaperna som möjliggörs av kvantmekaniken. Skulle en kvantdator kunna lösa heltals-faktorisering i polynomiell tid så skulle en stor del av världens säkerhets- och banksystem bli helt vidöppna för en attack. Än så länge är dagens kvantdatorer långt ifrån den storleksordningen på talen som behövs, rekordet idag med Shors algoritm är faktoriseringen av talet 21 [22]. En snabb utveckling inom kvantdatorer skulle således kunna ha en potentiellt stor icke-önskvärd påverkan på världens säkerhetsinfrastruktur.

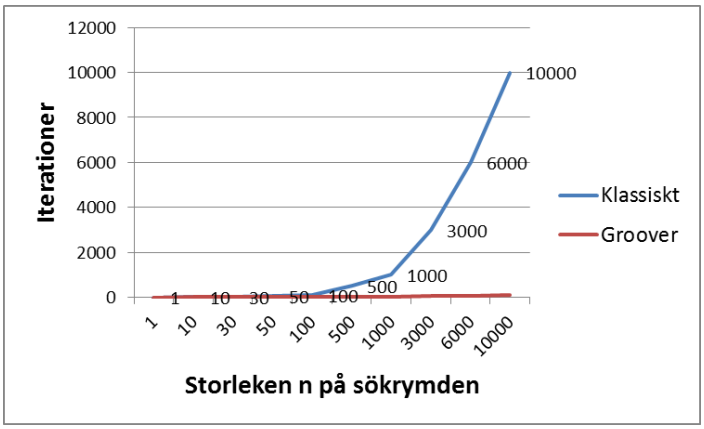
3.1.2.3 Grovers sökalgoritm

Att söka i en databas är ett centralt problem inom datavetenskap. Idag gör datorn ungefär som en människa gör när denne söker, ska man hitta ett telefonnummer eller en textsträng i en *osorterad* databas måste man gå igenom rad för rad. När databasen gås igenom ökar sannolikheten att hitta det man letar med en konstant vid varje iteration (eftersom sökrymden minskar med ett vid varje prövad lösning). Maximalt tar det alltså n sökningar innan sökningen hittar det man letar efter där n är antalet instanser i databasen. Man kan också skriva det som att tiden att lösa är n=1/p, där p är sannolikheten att hitta lösningen vid varje enskild iteration, t.ex. om sannolikheten är 50% så måste man försöka 1/0.5 = 2 gånger innan man lyckas. Klassiskt tar det alltså tiden 1/p för att söka igenom en databas vilket stämmer bra med intuitionen.

Det man har lyckats bevisa för en kvantdator är att den här logiken inte alltid stämmer. Grover [25] visade att en kvantmekanisk sökalgoritm i snitt tar tiden $1/\sqrt{p}$. En liten missuppfattning är dock att Grovers algoritm söker igenom alla möjliga lösningar direkt (med andra ord skulle en operation räcka för att få fram

lösningen). Istället så itererar den över alla möjliga lösningar flera gånger och får fram en lösning men det krävs k =$1/\sqrt{p}$ iteration tills lösningen är både sannolik *och* maximalt sannolik. Om fler än $1/\sqrt{p}$ iterationer görs så går sannolikheten att få rätt svar ned, så man kan inte få bättre resultat genom att iterera fler gånger som man kanske intuitivt kan tro.

Förbättringen jämfört med den klassiska metoden att söka i siffor kan ses i Figur 7. Här framgår hur olika sannolikheter skalar och att vid mycket små sannolikheter som en på tiotusen blir antalet iterationer mycket lägre med en kvantdator.



Figur 7: Jämförelse mellan antalet iterationssteg för att utföra en sökning med en klassisk algoritm och Grovers sökalgoritm.

En starkt bidragande orsak till att Grovers algoritm var ett sådant genombrott var att en generalisering av Grovers sökalgoritm innebär att flera problem kan få samma ökning i lösningshastighet. Brassard, Hoyer, Mosca, Tapp visade att genom generaliserad Grover sökning (även kallad amplitudförstärkning) kan man uppnå samma ökning i lösningshastighet på många klassiska problem [26].

3.1.2.4 Bernstein-Vazirani

En kanske ännu mer spektakulär tillämpning av kvant-algoritmer är Bernstein-Vazirani algoritmen. Den kan lösa problem i endast ett steg där en klassisk dator behöver upp till $2^{n-1}+1$ steg. I Deutsch-Jozsa problemet ska det avgöras ifall en funktion som får n-bitar som indata och ger 0 eller 1 som svar, ger ett *konstant* svar (alltså bara 0:or eller 1:or) eller ger ett *balanserat* svar (hälften 0 och hälften 1). Det finns alltså inga andra alternativ än dessa två typer av funktioner. Så i bästa fall om man har fått 0 och 1 på de första två olika indata vet man att funktionen inte är konstant och därmed balanserad, men har de första fyra svaren varit 0 och antalet bitar är n=3 (2^3=8 olika möjligheter för indata) så kan man inte

avgöra förrän efter nästa iteration vad det är för typ av funktion. I värsta fall behövs alltså $2^{n-1}+1$ steg för en klassisk algoritm för att avgöra typen av funktion. Det Bernstein-Vaziranis algoritm gör är att använda konstruktiv och destruktiv interferens i endast ett steg för att avgöra vilken typ av funktion det är, och till skillnad från t.ex. Grovers algoritm (som bara är *sannolikt* korrekt) är lösningen alltid korrekt [27].

3.2 Att bygga en kvantdator

DiVincenzo publicerade år 2000, [18], [28], [29] en förteckning över kriterier som måste vara uppfyllda för att realisera en skalbar kvantdator. Kriterierna är följande fem punkter

1. En skalbar implementering av ett två-nivå system för skapandet av kvantbitar.
2. Effektiva metoder för att initiera kvantbitarna i ett känt kvanttillstånd.
3. En universell uppsättning av grindar för att manipulera kvantbitarna.
4. Metoder för att mäta individuella kvantbitar.
5. En lång minnestid för att kunna spara kvantbitar.

Dessa kriterier utvidgas oftast till att omfatta två kommunikationskriterier [18], [28]

6. Förmågan att konvertera mellan stationära och flygande kvantbitar (atomer till fotoner).
7. Möjlighet att överföra kvantbitar mellan två platser.

Dessa sju kriterier har demonstrerats var för sig med många olika kvantsystem men än har inte alla delarna kunnat fogas samman på ett skalbart sätt. Svårigheten ligger dels i att kvantmekaniska system är oerhört sköra men också på att det finns många val på både beräkningsmodeller för kvantdatorer och fysikaliska system för implementering. Av dessa val är det inte säkert att endast en teknologi kommer bana vägen till den slutgiltiga implementeringen. Forskare har börjat undersöka möjligheten att kombinera olika teknologier för att nå skalbarhet[x] [30].

Ett avgörande krav för att kunna förverkliga en kvantdator är isoleringen av kvantsystemet. Punkt 1 i DiVincenzo kriterierna har länge varit forskningens primära fokus dels för att utveckla metoder för att isolera kvantbitarna från omgivningen och dels för att finna metoder för att effektivt manipulera (punkt 2 och 3) och mäta kvantbitarna (punkt 4).

[x] Se t.ex. projektet för en skalbar jondator på: www.quantum.gatech.edu/musiqc.shtml

Dekoherens, som är samlingsnamnet för störningar som förstör kvanttillstånd, orsakas av omgivningen och kommer av ett flertal olika effekter vilka beror mycket på det kvantmekaniska system som används. Till exempel kan en foton i en optisk fiber absorberas vilket medför en direkt förlust av kvantbiten eller kan dess polarisationsriktning roteras på grund av mekaniska förändringar i fibern. Med en aktiv polarisationskompensering av fibern kan rotationen av kvantbiten minimeras. Förlusten av fotoner är än ett olöst problem. För andra kvantbits teknologier uppkommer andra problem som exempelvis termiska fluktuationer som måste dämpas genom att kyla kretsen till temperaturer i storleksordningen tusentals grad över absoluta nollpunkten [31]. Nästan alla teknologier behöver kylas och isoleras kraftigt och därför behövs mycket utrustning för att skydda det lilla utrymmet som huserar kvantbitarna. Detta gör att de flesta kvantdatorteknologier kräver skrymmande utrustning som är främst till för isolation. Implementeringen av kvantbitarna är i sig ofta i storleksordningen mikrometer eller strax under vilket är relativt stora konstruktioner jämfört med dagens transistorer som är nere på nanometerskala.

Två tekniker som inte har samma strikta krav på nedkylningen är teknologier baserade på fotoner och NV-centra (kväve-hål defekter i diamant, nitrogen-vacancy in diamond). Fotoner reagerar svagt med sin omgivning vilket är åtråvärt men de är relativt ”stora”[y] vilket medföra att teknologin kommer vara svår att miniatyrisera. Diamantstrukturen runt NV-centrat ger kvantbiten ett visst skydd och med rätt filtering kan koherens observeras även i rumstemperatur. Men för att nå hög koherens måste även dessa kylas, dock inte like kraftigt som många andra teknologier.

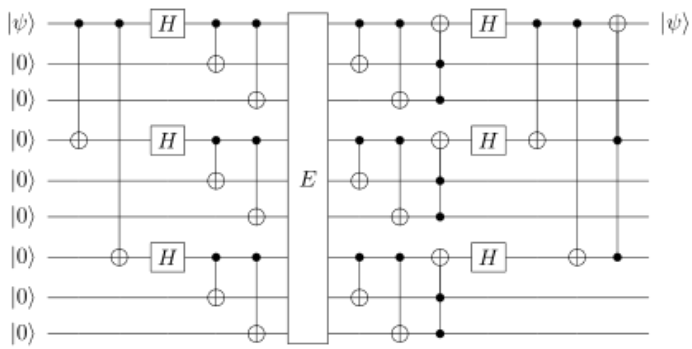
3.2.1 Felkorrigering

En viktig del av utvecklingen för kvantdatorn är felkorrigering. Kvanttillståndens sköra natur kommer att resultera i många fel under en körning. Att eliminera alla felkällor och få kvantdatorn att prestera lika felfritt som dagens datorer anses inte troligt. Därför är felkorrigering en mycket viktig del av kvantdatorimplementeringen [7]. Att felkorrigering över huvudtaget var möjligt att utföra på en kvantdator var framtill 1995 osäkert. Det året visade Peter Shor och Andrew Steane att möjligheten fanns genom att koda in informationen av en kvantbit i flera kvantbitar. Figur 8 illustrerar en algoritm som kan rätta fel som uppstår i någon av de nio kvantbitarna. Problemet med felkorrigering är att resurser förbrukas och om felen uppkommer allt för ofta kommer all datorkraft att gå åt. Därför är det viktigt att toleransen för felen som uppstår i

[y] Stora i avseendet att de optiska ledningarna i de komponenterna som används för att guida fotoner (optiska fiber och på optiska kretsar) har tjocklekar som är i storleksordningen tiotals mikrometer.

kvantdatorimplementeringen skalar fördelaktigt för uppgiften. Forskning i ämnet är central för skapandet av kvantdatorn och flera olika typer av felkorrigeringsmetoder och analysverktyg av feltoleransen har tagits fram sedan 1995 [32].

Konsekvensen av feltoleranta beräkningar och möjligheten att dynamiskt kunna rätta felen som uppkommer är mycket viktiga resultat. Idén om feltolerans i beräkningar är inget nytt utan utvecklades tidigt för klassiska datorer [33]. Konceptet bygger på att om ett fel uppstår ska felet inte sprida sig och bli större då beräkningen fortlöper. För kvantdatorn innebär detta att feltoleranta block kan designas för att utföra vissa delar av beräkningen och om ett fel uppstår rättas felet efter blocket innan nästa block tar vid. Innebörden är att om felsannolikheten ligger under ett tröskelvärde kan felen som skapas kontrolleras och skalning är då möjligt [32]. Tröskelvärdena beror på felkorrigeringskoden och modellen av det fysikaliska system som förväntas implementera den feltoleranta koden. De första felkorrigeringsmetoderna var fokuserade på att utveckla kodsystem för att på ett generellt sätt rätta felen som uppstod. Inriktningen har sedan dess skiftat mot ett mera applikationsnära felkorrigeringssystem där modeller av den fysikaliska implementeringen används för att öka möjligheterna till korrigering.



Figur 8:Illustration[z] av den grindbaserade beräkningsmodellen. Till vänster representeras initialiseringen av kvantbitarna som kommer in i kretsen. Kvantbitarna propagerar sedan genom nätverket av grindar (från vänster till höger) för att slutligen ge svarsresultatet via en mätning som inte syns i bilden. Kretsen som visas beskriver Shors felkorrigeringskod för en kvantbit som passerar igenom ett område E som kan orsaka ett fel. De lodrätta strecken med en prick motsvarar CNOT grindar, de med två prickar är Toffoli-grindar och H är Hadamard grindar.

[z] Bild från en.wikipedia.org/wiki/Quantum_error_correction

3.2.2 Beräkningsmodeller för kvantdatorer

En beräkningsmodell beskriver plattformen för hur informationen, som är inkodad i kvantbitarna, manipuleras för att utföra en beräkning. Själva tekniska implementeringen måste sedan följa DiVincenzo kriterierna för att beräkningen ska kunna genomföras.

3.2.2.1 Den grindbaserade beräkningsmodellen

Den mest studerade beräkningsmodellen är den som baserar sig på grindar [7]. Mycket likt de logiska grindarna som ligger till grund för beräkningarna i en klassisk dator kan grindar definieras för kvantdatorn. Dessa grindar beskriver enkla operationer som t.ex. NOT grinden som ändra en kvantbits basvektor från $|0\rangle$ till $|1\rangle$ och vise versa. Andra grindar som tar två eller fler kvantbitar kan även konstrueras. Ett exempel är CNOT (control NOT) grinden som utför en NOT operation på ena kvantbiten bara om den första, kontroll biten, är i $|1\rangle$ tillståndet. CNOT grinden kallas även ibland för en snärjelseskapande grind eftersom den skapar interaktionen som behövs för att förverkliga icke-klassiska korrelationer mellan kvantbitar. Likt en klassisk datorberäkning som kan beskrivas med en långserie uppbyggd av ett fåtal olika grindtyper kan kvantberäkningar delas upp i en serie byggd av ett fåtal grindtyper. En sådan är kombinationen av en generell rotation av kvantbiten tillsammans med CNOT grinden [34]. Det som karakteriserar denna beräkningsmodell är att varje grind är en fysikalisk process som processar kvantbitarnas inkodade information från grind till grind.

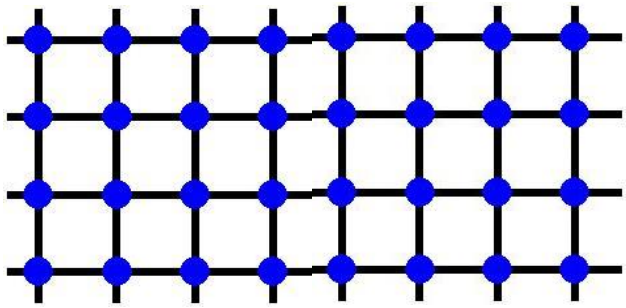
3.2.2.2 Envägs-kvantdatorn

En annan beräkningsmodell där kvantbitarna inte flödar igenom kretsen som i den grindbaserade modellen är istället snärjelsebaserad [35]. I denna beräkningsmodell skapas först ett specifikt kvanttillstånd, ett klustertillstånd (av engelskans cluster state även kallad graf state). Kvanttillståndet kan illustreras som grafer där varje korsning representerar en kvantbit och länkarna mellan representerar snärjelsen, se Figur 9 för ett specialfall som representerar ett rutnät.

Rutnätet skapar ett bräde där kretsar kan skapas genom att mäta på kvantbitarna som inte ska vara med i kretsen. Mätningen förstör länkarna mellan kvantbitarna och en krets karvas fram ur snärjelsen. När kretsen ska användas initialiseras den första kolumnen med kvantbitar i starttillstånden och sedan utförs en serie mätningar kolumn för kolumn. Mätprocessen tvingar fram informationen tills den når sista kolumnen som motsvarar svaret på beräkningen.

Eftersom beräkningen baserar sig på korrelationerna mellan kvantbitarna kommer kretsen att ha förstörts efter en genomförd beräkning. Samma grindar som i den grindbaserade modellen kan skapas genom att mäta på klustertillståndet. Detta gör att dessa två är beräkningsmässigt ekvivalenta. Nackdelen med modellen är att stora klustertillstånd måste skapas och hållas isolerade från störningar under hela initialiseringen och under mätprocessen.

Fördelen är att specialdesignade kretsar kan byggas och efter en körning kan beräkningen fortsätta genom att en ny krets skapas där resultaten av den gamla matas in i den nya.



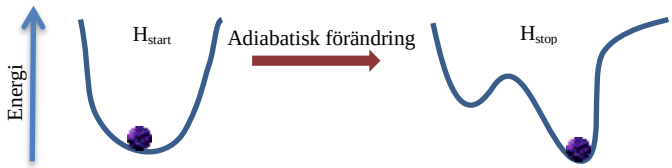
Figur 9: Envägs-kvantdatorn kan beskrivas med ett snärjt kvanttillstånd som representerar ett rutnät[å]. Varje blå punkt är en kvantbit och kopplingarna mellan dessa representerar snärjelse.

3.2.2.3 Adiabatisk kvantdator

En beräkningsmodell som skiljer sig märkbart från de två första är den adiabatiska beräkningsmodellen. Även denna har visat sig vara ekvivalent till den grindbaserade modellen, så när som på en liten skillnad i effektivitet. Beräkningsprincipen baserar sig på det adiabatiska teoremet som säger att: *ett kvanttillstånd kommer behålla sitt energitillstånd om en given störning sker tillräckligt sakta och det finns ett gap mellan energitillståndet och resten av energitillstånden som beskriver kvantsystemet.*

För att utföra en beräkning identifieras först en modell för hur kvantssystemets energi beror av systemets tillstånd. Modellen konstrueras så att det tillståndet med den lägsta energinivån motsvarar svaret på det problem som man vill lösa. Sedan initialiseras ett kvantsystem i grundtillståndet av en enkel modell för systemets energi. Genom att sakta transformera den enkla modellen för systemets energi till den mer komplexa kommer kvanttillståndet, på grund av adiabatiska teoremet, vara kvar i grundtillståndet under hela transformationen. Efter transformationen kommer kvanttillståndet att representera lösningen på problemet. Denna modell är inte lika väl studerad som den grindbaserade och många frågor kvarstår. Till exempel vilken roll har snärjelse och hur ska felkorrigerande koder kunna implementeras. Trots detta har flera försök gjorts för att implementera denna modell, mest känt är företaget D-wave systems försök till storskaliga beräkningar med upp till 512 kvantbitar.

[å] Bild från Wikipedia Commons



Figur 10: Adiabatisk beräkningsmodell. Landskapet förändras sakta via ett adiabatiskt förlopp. Under transformationen kommer kvanttillståndet, lila bollen, att hålla sig i den lägsta positionen om den startade i den lägsta positionen. Detta sker oavsett hur komplicerat slut kurvan än blir.

3.3 Teknologier

Vi presenterar här några teknologier som kan vara intressanta kandidater för implementering av en kvantdator. Dessa är ett litet urval av många teknologier som visar på bredden av uppfinningsrikedom och svårigheterna. För en fördjupning rekommenderar vi följande artiklar [36], [37], [31], [38], [39], [5], [40].

3.3.1.1 Jondatorn

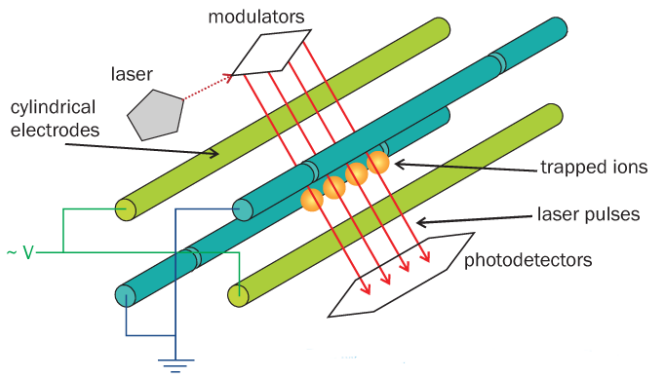
Av alla försök till en implementering är jondatorn [5] kanske den mest lovande. En jon är en atom som har tappat en elektron eller som har fått en extra elektron och därför är elektriskt laddad. Datorarkitekturen bygger på att hålla joner fångade i en fälla där de kyls ner, under mycket högt vakuum, till nära absoluta nollpunkten med hjälp av laserkylning, se Figur 11. Oftast används alkalimetaller eller vissa övergångsmetaller eftersom laserkylning kräver mycket specifika atomstrukturer för att fungera. En kvantbit representeras av två elektrontillstånd i jonen och genom laserpulser kan initialisering och detektion ske med nästan 100% effektivitet. Med laserpulser kan även andra operationer för en kvantbit utföras. För att implementera grindar mellan två kvantbitar används jonernas laddning.

Med denna teknik har snärjda tillstånd med hög kvalitet för ett fåtal joner demonstrerats. Hastigheten som grinden kan operera i är beroende av antalet joner i fällan och skalar som $1/\sqrt{n}$, där n är antalet joner. På grund av detta har varje jonfälla en begränsad kapacitet mellan 10-100 joner där merpartern av experimenten arbetar med 10 till 20 joner. Tekniken är nu inne i skedet att dels kunna effektivt adressera jonerna och dels utföra grindarna korrekt.

Framförallt görs stora insatser för att hitta skalningsmetoder för att adressera fler joner. Flera metoder har förslagits, bland annat mikrofällor[ä] där det är möjligt att

[ä] http://www.quantum.gatech.edu/musiqc.shtml

slussa joner mellan olika fällor på ett mikrochip. En annan riktning är att sammanbinda flera separerade fällor genom att snärja en jon med en foton som används sedan i en typ av kvantteleportering för att skapa snärjelse mellan separerade fällor. Metoden är mycket lik idén om kvantupprepare som diskuterades i kvantkrypteringskapitlet och möjliggör att två separerade jonfällor kan kommunicera med varandra.



Figur 11: Illustration av en jonfälla[ö], de oranga bolarna motsvarar joner som hålls på plats genom elektriska fält som skapas av strömmen i de fyra ledarna. Jonerna bildar ett pärlband eftersom de stöter bort varandra. Med laserljus kyls och manipulerar kvantbitarna.

3.3.1.2 Fotonbaserad kvantdator

Fotoner har många fördelar för implementering av en kvantbit. Framförallt kan fotonen färdas långa sträckor utan att dekoherera och är idag de enda realistiska alternativet för långdistans kvantinformationsöverföring. Egenskapen att endast reagera med sin omgivning på ett linjärt vis gör fotonen till ett självisolerande system som uppvisar kvantegenskaper utan att behöva allt för sofistikerad utrustning. Denna mycket attraktiva egenskap är dessvärre också dess svaghet eftersom två fotoner inte påverkar varandra märkvärt.

Som kvantbit är polarisation den mest direkta implementeringen. Flera andra system har föreslagits men polarisation är så pass enkelt att rotera, preparera och

[ö] Bild från Wikipedia Commons

mäta att den är i de flesta fallen att föredra. Kvantgrindar för en polarisationsinkodad kvantbit är enkla att utföra med dubbelbrytande material som exempelvis kvarts, kalkspat, flytande kristaller (LCD) och genom en ren mekaniskt eller termiskt deformation av en optisk fiber.

Den stora nackdelen med fotoner är att de grindar som kombinerar flera kvantbitar inte kan skapas på ett enkelt sätt. Med linjära optiska komponenter, så som stråldelare för interferens, polarisationsutrustning och detektorer, kan grindar för två fotoner skapas men dessa har låg effektivitet och skalar dåligt. Att fotoner ses som en kandidat till kvantdatorn är framförallt på grund av ett genombrott av Knill, Laflamme och Milburn som visade 2001 att optik med en-fotonkällor och fotonräknande detektorer kan användas för att realisera en skalbar kvantdator [41], [42]. Men det har visat sig vara komplicerat att utföra större beräkningar och bara mindre proof-of-concept experiment har hittills demonstrerats. Största begränsningen är idag att förslaget behöver effektiva detektorer som kan urskilja fotonantalet och väl fungerande en-fotonkällor. Dessa ska sedan kunna integreras i vågledare i en integrerad optikkrets med elektronik för frammatning av signalen eftersom varje grind kommer att behöva flera detektorer och extra fotoner för att få effektiva grindar mellan fotoner. Att kombinera alla dessa steg är långtifrån trivialt och forskargrupper har bara börjat experimentera med de olika teknologierna.

3.3.1.3 Supraledande kvantbitar

Elektriska kretsar med komponenter ses ofta som system som lyder under den klassiska fysiken. Skapas komponenterna av supraledande[aa] material med låga förluster kommer den klassiska fysiken inte att räcka till och beskrivningen måste göras med hjälp av kvantmekanik. Grundkomponenterna som behövs för en kvantdator är kondensatorer, induktorer, Josephson[bb]-barriärer och hålrumsresonatorer[cc]. Första steget till att skapa en kvantbit är att skapa en kvantmekanisk harmonisk oscillator, detta kan göras med en svängningskrets som består av en kondensator och en induktor vilket skapar en LC-krets. För en klassisk LC-krets kommer strömmen att pendla mellan kondensatorn och induktorn vid en given resonansfrekvens. Energin kommer att pendla mellan att vara i laddningspotential i kondensatorn och i det magnetiska fält som finns runt induktorn.

[aa] Supraledande material har egenskapen att elektroner i ledningen inte har något motstånd utan flödar friktionsfritt.

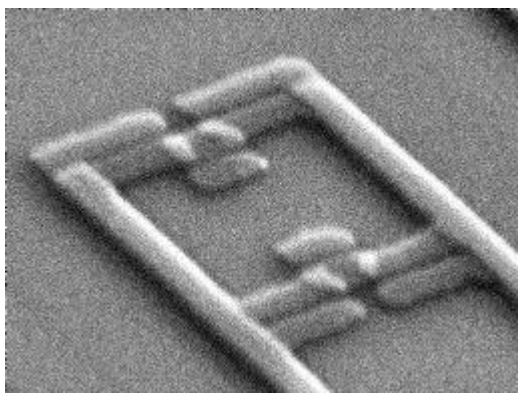
[bb] Josephson-effekten är en tunnelström som sker då två supraledande ytor separeras med ett tunt isolerande material. Josephson barriären ger en icke-linjär effekt till kretsen utan att dekoherera kvanttillståndet.

[cc] Hålrumsresonatorer fungerar dels som bandbasfilter men också som en koherent koppling mellan kvantbitar, frekvensstabilisering för kvantbitar och minne.

Den kvantmekaniska beskrivningen behövs när kretsen kyls till omkring tjugo tusendels grad över absoluta nollpunkten och samtidigt är magnetiskt och elektriskt isolerad. I kvantversionen kommer kretsen att ha energitillstånd som är jämnt fördelade. Energinivåerna kan användas för implementeringen av en kvantbit, men eftersom dessa är separerade med en fix frekvens kommer det vara svårt att isolera två nivåer från varandra. För att bryta symmetrin används en Josephson barriär som ändrar energidistributionen så att energinivåerna inte länger är separerade av en fix frekvens. De två lägsta nivåerna kan sättas så att de är separerade av en unik frekvens, vilket medför att dessa två nivåer kan adresseras separat. Flexibiliteten i designen gör att dessa kretsar ibland kallas artificiella elektroniska atomer.

Fördelen med denna teknologi är att alla komponenter kan tillverkas med litografiska metoder från modern mikroelektroniktillverkning. Detta möjliggör skalning där komplexa konstruktioner med många kvantbitar kan skapas relativt enkelt. På grund av detta har två företag, IBM och D-wave systems, valt denna inriktning.

Likt andra kvantmekaniska teknologier kämpar forskargrupper med att få kvantbitarna att inte förlora sina kvantmekaniska egenskaper och att få dem att reagera med varandra på ett kontrollerbart sätt. Experimenten som har gjorts är framförallt baserade på kretsar med upp till 5 kvantbitar där bra kontroll har demonstreras. Men med detta sagt finns det storskaliga ”experimentet” D-wave som har chip med 512 kvantbitar, men dessa är inte lika väl studerade och det är inte säkert hur väl kvantbitarna kan snärjas till varandra.



Figur 12: En svepelektronmikroskopbild[dd] av en supraledande kvantbit.

[dd] Bild från: http://en.wikipedia.org/wiki/File:Flux_Qubit_-_Holloway.jpg

3.3.1.4 D-wave

År 1999 startade företag D-wave systems[ee] med målet att skapa den första kommersiellt tillgängliga kvantdatorn [43]. Ambitionen var inte att sträva efter en universell kvantdatorarkitektur baserad på logiska grindar utan att istället sikta på en adiabatisk kvantdator, se kapitel 3.2.2.3, som implementerar en viss klass av problem. Den klass av energimodeller som implementerades var för att lösa kombinatoriska optimeringsproblem. Detta inkluderar problem som t.ex. den resande försäljaren och optimering av Ising-modellen som är en viktig modell inom fysiken. Exempel på algoritmer som inte kan utföras är Shors faktoriseringsalgoritm, se kapitel 3.1.2.2. D-wave är därför inte en generell kvantdator utan är specialiserad för en viss klass av problemställningar.

Företaget har fått mycket publicitet de senaste åren på grund av att NASA tillsammans med Google och USRA (Universities Space Research Association) har köpt ett system, se Figur 13. Även Lockheed Martin har inskaffat ett system som de uppgraderade under 2013 till en 512 bits version. Trots dessa framgångar har det vetenskapliga samfundet varit skeptiska till D-wave systemet[ff]. Detta framförallt för att företaget inte kunnat visa att systemet kan utföra beräkningar som demonstrerar på storskalig kvantmekanisk förmåga.

Nyligen (i slutet av januari) har forskare från Berkeley och IBM visat [44] att ett av de starkare argumenten för att D-wave har en förmåga att kunna bearbeta information på ett storskaligt kvantmekaniskt vis kan modelleras genom en klassisk datormodell. Slutsatsen var att de datorgenererade korrelationerna var minst lika bra som de som produceras av D-wave datorn. Detta kontrades med en publikation (kom ut i slutet av maj) där ett bevis för att 8 kvantbitar i D-wave är snärjda med varandra men dessa kvantbitar ligger nära varandra och därför kan vara en lokal effekt [45]. En snabb och het debatt förs kontinuerligt mellan D-wave och andra forskare men än behövs mer data för att verkligen visa kvantdatorkapacitet. En av de större skeptikerna är Scott Aronson på MIT som länge har bloggat i ämnet[gg]. Även svenska forskare har uttalat sig skeptiska till D-waves påståenden, till exempel i en intervju[hh] för Sveriges Radio uttalar sig Göran Johannson på Chalmers om risken för minskad finansiering inom ämnet.

Ytterligare en kritik riktad mot D-wave är att programmeringen av datorn kräver en mycket komplicerad ombearbetning av problemställningen för att passa datorarkitekturen. Det är alltså fortfarande under debatt om D-wave kan

[ee] Hemsida: www.dwavesys.com/

[ff] Två diskussioner om D-wave:
www.ibm.com/developerworks/community/blogs/jfp/entry/will_quantum_computing_kill_cplex
www.scottaaronson.com/blog/?p=1400

[gg] www.scottaaronson.com/blog/?p=1400

[hh] http://sverigesradio.se/sida/artikel.aspx?programid=104&artikel=5602093

klassificeras som en kvantdator eller om den är en ny arkitektur på en specialiserad klassisk dator för en viss typ av optimeringsproblem.

Teknologin som D-wave baserar sin datorarkitektur på är supraledande kvantbitar[ii], se kapitel 3.3.1.3. Kretsen är designat för att implementera QUBO (Quantum Unconstrained Binary Optimization) där optimeringen försöker minimera en funktion genom ”quantum annealing” vilket är en variant av den adiabatiska beräkningsmodellen. D-wave erbjuder nu även ett simuleringspaket, vilket ger en introduktion till hur systemet programmeras.

Valet av att implementera QUBO är enligt Geordie Rose (direktör för teknik, forskning och utveckling på D-wave) att problemet är NP-svårt att lösas och att den dessutom uppkommer i många fysikrelaterade problem som Ising-modellen. Ambitionen har varit att utveckla en ”analog dator” som arbetar på gränsen av vad som är möjligt. Sedan lanseringen 2002 av deras första system har företaget lyckats dubbla antalet kvantbitar varje år och är nu uppe i 512 kvantbitar. Denna trend, som de har namngett till Rose’s Law, är något som företaget eftersträvar att hålla. Strategin är att leverera system med allt fler kvantbitar och under tiden undersöka om den klarar av att klassificeras som en kvantdator.

I ett led i Googles kvantdatorsatsning lanserade de nyligen Quantum Computing Playground[jj] som är ett verktyg för att simulerar kvantalgoritmer.

Figur 13: Installation av NASA:s nya D-wave dator med 512 kvantbitar[kk].

[ii] Se Geordie Rose från D-wave berätta om hur systemet fungerar under ett Google konvent: www.youtube.com/watch?v=vMvC-wv1ayo

[jj] http://qcplayground.withgoogle.com/#/home

4 Bevakningsbehov

Kvantinformatik är ett relativt nytt ämne som spås kunna ha stor påverkan antingen direkt med skapandet av kvantdatorn eller indirekt med teknologier som skapas på grund av kapplöpningen att utveckla en kvantdator. Den snabba teknikutvecklingen gör att flera delar av fältet kvantinformatik är på väg mot kommersialisering med allt mer sofistikerade system.

4.1 Kvantkryptografi

Idag utförs mycket av forskningen av universitet och forskningsinstitut men företag har börjat nappa. Till exempel utvecklas nätverk dedikerade för kvantkryptering i flera länder såsom Österike, Kina, Frankrike, Australien och USA. Där finns även planer för satellitbaserade system för kommunikation mellan två avlägsna platser men även mellan satelliter. Detta har potential att ändra landskapet för vilka resurser som krävs vid spaning och underrättelseverksamhet. Idag har de kommersiella systemen begränsad räckvidd och flera säkerhetshål finns, men teknikutvecklingen går snabbt framåt och det förväntas att fler aktörer kommer att etablera sig med nya förbättrade system. Detta gör att en bevakning är nödvändig för att kunna följa utvecklingen och bedöma riskerna.

4.2 Kvantdatorn

Flera stora forskningscentra[ll] finns idag dedikerade till kvantinformation där ofta en av huvudinriktningarna är kvantdatorn. Kvantdatorns förmåga är idag inte väl förstådd men den har stor potential i många ämnen som har, om inte direkt, en nära relation till säkerhetsfrågor. Teknikutvecklingen relaterad till kvantdatorn har stor potential inte bara för beräkningsdelen utan också för nya typer av sensorer.

[kk] Bild “Googles first quantum computer” från: www.flickr.com/ creativecommons.org/licenses/by/2.0/

[ll] Några forskningscentra är, många fler finns: Frankrike (http://www.pcqc.fr/), England (http://oxfordquantum.org/), Kanada (https://www.perimeterinstitute.ca), Australien (http://www.cqc2t.org/), USA (http://qis.mit.edu/).

Redan idag har flera företag investerat i ett D-wave system som kanske inte fullt ut är en kvantdator. Men potentialen har fått företagen att lägga ut de närmare 10M$ som en sådan dator spekuleras kosta. Bevakningsbehovet av D-wave och andra kvantdatorteknologier är av intresse eftersom de har potential till att bryta ett av de vanligaste krypteringsprotokollen som används flitigt av bankväsendet. Bevakningsbehovet är inom både teoretiska och experimentella tekniker eftersom de är mycket beroende av varandra.

5 Säkerhetsaspekter

Här sammanfattar vi både kvantkryptografi och kvantdator avsnittet med hjälp av ett par teknikprognoser.

5.1 Kvantkryptograf

Kvantinformatikens första kommersiella applikation är kvantkryptografin. Flera företag är idag verksamma inom området men mycket av utvecklingen ligger än hos forskargrupper på universitet. Metoden hjälper i distributionen av korrelerade slumptal mellan två eller flera parter för användning i det klassiska engångskryptot. Fördelen med ett kvantmekaniskt system är att i distributionen av fotonerna ger den möjligheten att upptäcka om distributionslinan är avlyssnad.

Kvantmekanikens stokastiska natur gör den även intressant för enklare system som skapandet av lokala slumptalssekvenser med hög kvalitet. Företag som Idquantique har utvecklat pci-kort och USB-stickor för slumptals generering som kan användas i exempelvis Monte Carlo-simuleringar och inom spelindustrin.

5.1.1 Tekniktrend 1

Kommersialisering är igång med allt fler aktörer. På kort sikt kommer allt fler fiberbaserade system att demonstreras med allt större nätverk där inte endast två aktörer är inblandade. Även mindre handhållna mobila enheter kan vara tekniskt möjligt i framtiden. I nuläget är systemen ganska sårbara men för varje bugg och bakdörr som hittas försöker företagen att hitta korrigeringar. Räckviden är än så länge begränsad men forskningsinsatser läggs på att hitta nya metoder som ska förlänga avstånden. En möjlig lösning är utvecklingen av kvantuppreparen.

TRL: 6-8

5.1.2 Tekniktrend 2

Protokoll för kvanthemlighetsdelning som går utanför traditionell nyckeldelning förväntas också komma till kommersiella aktörer. Detta kräver dock att ett robust kvantvänligt nätverk utvecklas där flera parter kan koppla in sig. När ett nätverk av kvantupprepare finns tillgängligt kommer, troligtvis, protokoll som baserar sig på snärjelse att bli kommersialiserade. Ser vi ännu längre fram då robusta kvantminnen och kvantdatorer finns tillgängliga öppnas även möjligheten att utföra distribuerade kvantdatorberäkningar med ett sådant nätverk.

TRL: 1-3

5.1.3 Tekniktrend 3

Ett av de stora forskningsmålen är att demonstrera satellitbaserade länkar med snärjda fotoner. Här arbetar flera forskargrupper och de stora aktörerna finns i Europa, Kina och Kanada. Experimentella försök kommer troligtvis att komma inom en snar framtid eftersom Österike och Kina redan har uppskjutningsplaner till 2016[mm]. De första experimenten som kommer att utföras kommer att vara baserade på E91 protokollet och Bell-olikheter och inte långt efter kommer kvantteleportering att demonstreras. I förlängningen kommer stora insatser att läggas på att kunna spara partiklarna i kvantminnen för att kunna ackumulera snärjelse och utföra kvantbits operationer (t.ex. destillering) där flera kvantbitar måste reagera med varandra.

TRL: 1-3

5.1.4 Tekniktrend 4

Ett problem med kvantkrypteringstekniken är att tillverkaren måste var tillförlitlig. Det kan vara enkelt för en illasinad aktör att införa bakdörrar i systemen. Försök att minska detta beroende undersöks nu av flera forskargrupper. Vissa framsteg har gjorts på teorier som går bortom kvantmekaniken (kvantmekaniken kanske inte är den slutgiltiga teorin) där säkerhet garanteras inte bara av kvantmekanikens lagar men också av alla andra teorier som innefattar vissa typer av statistiska strukturer. T.ex. finns det protokoll som bara antar att information inte kan färdas snabbare en ljuset. Dessa protokoll baserar sig på de statistiska underlag som snärjelse ger och kommer endast bli tillgängliga när nätverkslösningarna har mognat till sådan grad att snärjelsen kan distribueras och destilleras tillförlitligt.

TRL: 1

[mm] http://www.nature.com/news/data-teleportation-the-quantum-space-race-1.11958
http://illvet.se/teknik/ubrydelige-koder-gaar-i-luften-i-i-2016

5.2 Kvantdatorn

Hur ställningen för kvantdatorutvecklingen är idag sammanfattas väl av slutorden i [18] där författarna skriver:

> Let us close with a question that provokes answers ranging from, "Already has," (in reference to direct quantum simulation of a specific quantum system) to "Twenty years," to "Never,"— and all these from people actually working in the field: When will the first paper appear in Science or Nature in which the point is the results of a quantum computation, rather than the machine itself? That is, when will a quantum computer do science, rather than be science?

Viktigt att inse är att kvantdatorn representerar en ny typ av beräkningshjälp som ger lösningsmetoder som inte är effektiva med en klassisk dator. Dvs. kvantdatorn är inte en superdator med extra mycket beräkningskraft utan något helt nytt. Kvantdatorns effektivitet kommer inte av att den gör fler beräkningar per sekund utan istället löses problemen genom att utnyttja möjligheter, via kvantfysiken, som inte på ett effektivt sett är tillgängliga för en klassisk dator. Dessa nya metoder finns tillgängliga eftersom den bearbetar ettor och nollor genom ett kvantmekaniskt regelverk där superposition och snärjelse spelar viktiga roller.

5.2.1 Tekniktrend 1

Mycket av kvantinformationsfältet ligger i utvecklingen av tekniker för att koherent manipulera partiklar. Än kan endast ett fåtal partiklar användas, t.ex. 8 fotoner, 12 joner eller 4 supraledande kretsar. Viss förhoppning finns i att försöka kombinera olika tekniker för att skala systemen till fler kvantbitar. För de närmaste 10 till 20 åren ser utvecklingen ut att domineras av demonstrationer som kommer att fokusera på att öka antalet kvantbitar, visa på mer robusta kvantminnen, effektivare konverteringsmetoder för att gå mellan olika kvantbitsteknologier, implementeringar av felkorrigerande koder och brushantering. Allt bygger på att hitta rätt teknologi för uppgiften.

TRL: 1

5.2.2 Tekniktrend 2

Kvantbitsteknologin med tillhörande grindar, minnen m.m. är grunden för kvantdatorn, men för att ha en fullt fungerande kvantdator behövs ytterligare flera lager av teknologier. Exempelvis i mjukvaruområdet behövs utveckling av nya kvantalgoritmer, programmeringsspråk, felkorrigering och komplexitetsteori. Denna utveckling går hand i hand med den grundläggande utvecklingen av

kvantbitsteknologin. Fram till nyligen har det varit svårt med samarbeten mellan de mer mjukvarubaserade delarna och de experimentella grundteknologierna. Men framstegen inom experimenten gör att allt mer komplexa system kan skapas och bli intressanta för mjukvaruutvecklarna.

TRL: 1

5.2.3 Tekniktrend 3

Kvantdatorn förväntas ha förmåga till beräkningseffektiva simuleringar av kvantmekaniska system. Utvecklingen av nya typer av material, kemiska egenskaper, optiska egenskaper, mekaniska egenskaper m.m kommer att vara av intresse för kvantdatorn. Alla fält där komplexa kvantprocesser är involverade kommer troligtvis att hjälpas. Detta kommer resultera i nya typer av förmågor från fält som begränsas i dagsläget av komplexa beräkningar och simuleringar.

TRL: 1

5.2.4 Tekniktrend 4

Med kvantdatorn kommer utvecklingen av helt nya analysverktyg för databehandling att accelerera. Områden som troligtvis kommer att ha nytta av kvantdatorn är artificiell intelligens, sökmotorer, mönsterigenkänning och simulering av väder, genetik och materialforskning. Vi är idag allt mer beroende av avancerade sökningar vilket är allt från en enklare internet-sökning till hur man ska vecka proteiner för att få specifika egenskaper. Andra exempel är mjukvaruverifiering, hitta primtalsfaktorer (bryta RSA-kryptot och försvaga AES-kryptot), hitta mönster i stora datamängder för sensorfusion, och hitta globala minima i optimeringsproblem. Gemensamt för de flesta problemen, som förväntas ha potential att lösas effektivt med en kvantdator, är att de kan reduceras till sökningar med många val för varje nivå.

TRL: 1

6 Litteraturförteckning

[1] R. P. Feynman, ”Simulating Physics with Computers,” *International Journal of Theoretical Physics* , vol. 21, p. 467, 1982.

[2] D. Deutsch, ”Quantum theory, the Church-Turing principle and the universal quantum computer,” *Appeared in Proceedings of the Royal Society of London,* vol. 400, pp. 97-117, 1985.

[3] S. Lloyd, ”Universal quantum simulators,” *Science,* vol. 273, p. 1073, 1196.

[4] C. E. Shannon, ”Mathematical theory of communication,” *The Bell system technical Journal,* vol. 27, p. 379, 1948.

[5] C. Monroe och J. Kim, ”Scaling the Ion Trap Quantum Processor,” *Science,* vol. 339, p. 1164, 2013.

[6] A. Einstein, B. Podolsky och N. Rosen, ”Can Quantum-Mechanical Description of Physical Reality be Considered Complete?,” *Phys. Rev.,* vol. 47, p. 777–780, 1935.

[7] M. A. Nielsen, Quantum Computation and Quantum Information, Cambridge University Press, 2010.

[8] P. Jonsson, ”Review of Free-Space Quantum Key Distribution,” *FOI,* pp. FOI-R--1165--SE, 2004.

[9] N. Gisin, G. Ribordy, W. Tittel och H. Zbinden, ”Quantum cryptography,” *Reviews of modern physics* , vol. 74, nr 1, p. 145, 2002.

[10] G. Brumfiel, ”Quantum cryptography: Seeking absolute security,” *Nature,* vol. 447, pp. 372-373, 2007.

[11] J.-P. Bourgoin, E. Meyer-Scott, B. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, N. Lütkenhaus, R. Laflamme och T. Jennewein, ”A comprehensive design and performance analysis of LEO satellite quantum communication,” *New. J. Phys.* , vol. 15, p. 023006 , 2013.

[12] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter och A. Zeilinger, ”Entanglement-based quantum communication over 144 km,” *Nature Physics* , vol. 3, pp. 481 - 486, 2007.

[13] J. Yin, Y. Cao, S.-B. Liu, G.-S. Pan, J.-H. Wang, T. Yang, Z.-P. Zhang, F.-M. Yang, Y.-A. Chen, C.-Z. Peng och J.-W. Pan, ”Experimental quasi-single-photon transmission from satellite to earth,” *Optics Express* , vol. 21, nr 17, p. 20032, 2013.

[14] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin och A. Zeilinger, ”Quantum teleportation over 143 kilometres using active feed-forward,” *Nature*, vol. 489, p. 269–273, 2012.

[15] N. Gisin, S. Kröll, W. Scholer, J.-L. l. Guoet, P. Goldner och G. Ribordy. [Online]. Available: http://cordis.europa.eu/fp7/ict/photonics/docs/factsheets/qurep-flyer_en.pdf.

[16] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio och V. Scarani, ”Device-Independent Quantum Key Distribution,” [Online]. Available: http://www.secoqc.net/. [Använd 24 04 2014].

[17] A. Acín, S. Massar och S. Pironio, ”Efficient quantum key distribution secure against no-signalling eavesdroppers,” *New Journal of Physics*, vol. 8, nr 126, 2006.

[18] R. V. Meter och C. Horsman, ”A Blueprint for Building a Quantum Computer,” *Communications of the ACM*, vol. 56, nr 10, pp. 84-93, 2013.

[19] P. Shor, ”Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer (Revised version of the 1994 original),” *SIAM J. Comput.*, vol. 5, nr 26, p. 1484–1509, 1997.

[20] J. Simon, W. S. Bakr, R. Ma, M. E. Tai, P. M. Preiss och M. Greiner, ”Quantum simulation of antiferromagnetic spin chains in an optical lattice,” *Nature* , nr 472, pp. 307-312, 2011.

[21] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood och I. L. Chuang, ”Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance,” *Nature*, vol. 414, p. 883, 2001.

[22] E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X. Q. Zhou och J. L. O'Brien, ” Experimental realization of Shor's quantum factoring algorithm using qubit recycling.,” *Nature Photonics*, vol. 6, nr 11, pp. 773-776, 2012.

[23] R. P. Poplavskii, ”Thermodynamical models of information processing,” *Sov. Phys. Usp.*, vol. 3, nr 115, p. 465–501, 1975.

[24] J. W. Britton, B. C. Sawyer, A. C. Keith, C.-C. J. Wang, J. K. Freericks, H.

Uys, M. J. Biercuk och J. J. Bollinger, ”Engineered two-dimensional Ising interactions in a trapped-ion quantum simulator with hundreds of spins,” *Nature,* nr 484, p. 489–492, 2012.

[25] L. K. Grover, ”Quantum mechanics helps in searching for a needle in a haystack.,” *Physical review letters,* vol. 2, nr 79, p. 325, 1997.

[26] G. Brassard, P. Hoyer, M. Mosca och A. Tapp, ”Quantum amplitude amplification and estimation,” *Arxiv,* pp. quant-ph/0005055, 2000.

[27] D. Deutsch och R. Jozsa, ”Rapid solutions of problems by quantum computation,” *Proceedings of the Royal Society of London A,* p. 439: 553, 1992.

[28] D. DiVincenzo, ”The physical implementation of quantum computation,” *Fortschritte Der Physik-progress Phys.,* vol. 48, nr 771, pp. 9-11, 2000.

[29] D. P. DiVincenzo, ”Quantum Computation,” *Science,* vol. 270, nr 5234, pp. 255-261, 1995.

[30] C. Monroe, R. Raussendorf, A. Ruthven, K. R. Brown, P. Maunz, L. Duan och J. Kim, ”Large Scale Modular Quantum Computer Architecture with Atomic Memory and Photonic Interconnects,” *Arxiv,* p. arXiv:1208.0391v2, 2013.

[31] T. D. Ladd1, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe och J. L. O’Brien, ”Quantum computers,” *Nature,* vol. 464, nr 4, p. 45, 2010.

[32] S. J. Devitt, W. J. Munro och K. Nemoto, ”Quantum Error Correction for Beginners,” *Arxiv,* p. arXiv:0905.2794v4, 2013.

[33] J. V. Neumann, ”Probabilistic logics and the synthesis of reliable organisms from unreliable components.,” *Automata Studies,* p. 43, 1955.

[34] C. Williams, Explorations in Quantum Computing, London : Springer-Verlag , 2011.

[35] R. Raussendorf och H. J. Briegel, ”A One-Way Quantum Computer,” *Physical Review Lettes,* vol. 86, nr 22, p. 5188, 2001.

[36] M. Steffen, D. P. DiVincenzo, J. M. Chow, T. N. Theis och M. B. Ketchen, ”Quantum computing: An IBM perspective,” *IBM J. RES. & DEV.,* vol. 55, nr 5, 2011.

[37] J. Stajic, ”The Future of Quantum Information Processing,” *Science,* vol. 339, p. 1163, 2013.

[38] D. D. Awschalom, L. C. Bassett, A. S. Dzurak, E. L. Hu och J. R. Petta, ”Quantum Spintronics: Engineering and Manipulating Atom-Like Spins in Semiconductors,” *Science,* vol. 339, p. 1174, 2013.

[39] M. H. Devoret och R. J. Schoelkopf, ”Superconducting Circuits for Quantum Information: An Outlook,” *Science,* vol. 339, p. 1169, 2013.

[40] A. Stern och N. H. Lindner, ”Topological Quantum Computation—From Basic Concepts to First Experiments,” *Science,* vol. 339, p. 1179, 2013.

[41] E. Knil, R. Laflamme och G. J. Milburn, ”A scheme for effcient quantum computation with linear optics,” *Nature,* vol. 409, p. 46, 2001.

[42] A. J. F. Hayes, A. Gilchrist, C. R. Myers och T. C. Ralph, ”Utilizing encoding in scalable linear optics quantum computing,” *J. Opt. B,* vol. 6, p. 533, 2004.

[43] N. Jones, ”The Quantum Company,” *Nature,* vol. 498, p. 286, 2013.

[44] S. W. Shin, G. Smith, J. A. Smolin och U. Vazirani, ”How "Quantum" is the D-Wave Machine?,” *Arxiv,* p. arXiv:1401.7087v2, 2014.

[45] T. Lanting och m.m., ”Entanglement in a Quantum Annealing Processor,” *Physical Review X,* vol. 4, p. 021041, 2014.

[46] R. Horodecki, P. Horodecki, M. Horodecki och K. Horodecki, ”Quantum entanglement,” *Arxiv,* nr arXiv:quant-ph/0702225v2, 2007.

[47] H. Bombin, R. Andrist, M. Ohzeki, H. Katzgraber och M. Martin-Delgato, ”Strong Resilience of Topological Codes to Depolarization,” *Phys. Rev. X.,* p. 2:021004, 2012.

[48] Y.-M. He, Y. He, Y.-J. Wei, D. Wu, M. Atatüre, C. Schneider, S. Höfling, M. Kamp, C.-Y. Lu och J.-W. Pan, ”On-demand semiconductor single-photon source with near-unity indistinguishability,” *Nature Nanotechnology,* vol. 8, pp. 213-217, 2013.

[49] T. Ralph, A. Gilchrist, G. Milburn, W. Munro och S. Glancy, ”Quantum computation with optical coherent states,” *HP Laboratories Bristol,* pp. HPL-2003-124, 2003.

Kvantinformatik är ett relativt nytt ämne som har sina rötter i fysikens värld. Under början av 1900-talet presenterades flera nya koncept inom fysiken som slutligen kulminerade med den kvantmekaniska teorin. Trots sina stora framgångar att förutsäga experimentella resultat startade en debatt om hur väl teorin egentligen speglar verkligheten. Debatten kretsade kring att den kvantmekaniska teorin har flera svårsmälta ingredienser i sig som strider mot den klassiska världsbild vi är vana vid. Dessa fenomen, till exempel superpositionsprincipen (saker och ting kan befinna sig på flera ställen samtidigt), vågpartikeldualismen (partiklar beter sig som vågor och vågor som partiklar) och snärjelse (starka korrelationer mellan partiklar), kom att visa sig ha stor potential inom både kryptografi och datavetenskap.

Kvantinformatik är ett tvärvetenskapligt ämne där kvantfysik möter informationsteori. Två delar inom ämnet, kvantkryptografi och kvantdatorn, är mer applikationsinriktade och kan potentiellt ha stora konsekvenser för samhälle, försvar och säkerhet. Rapporten fokuserar på att ge en överblicksbild där vi belyser statusen idag, pågående teknikutveckling och prognoser över vilka medel som kommer kunna var tillgängliga i framtiden. I denna rapport beskrivs de delar av kvantinformationsfältet som är relaterat till kvantkryptografi och kvantdatorer. Syftet är att ge läsaren en inblick i de olika teknikerna, framstegen, potentialen, och dess begränsningar.

FOI

ISSN1650-1942

www.foi.se