Bundesamt
für Sicherheit in der
Informationstechnik

Entwicklungsstand Quantencomputer

Deutsche Zusammenfassung

BSI-Projektnummer 283

Änderungshistorie

Version	Datum	Name	Beschreibung
1.0	Mai 2018		Abschluss der Hauptphase des Projekts

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582 0
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de
© Bundesamt für Sicherheit in der Informationstechnik 2018

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Zusammenfassung

1.1 Was ist ein Quantencomputer?

Heutige Computer behandeln Informationen gemäß den Gesetzen der klassischen Physik: Register und Speicherinhalte haben zu jedem Zeitpunkt einen einzigen Wert. Dies gilt ungeachtet der Tatsache, dass die Bauelemente eines Computers wie Transistoren auf den Gesetzen der Quantenphysik basieren.

In einem Quantencomputer wird die Information selbst quantenmechanisch behandelt: Register und Speicherinhalte können mehrere Werte gleichzeitig in Überlagerung enthalten und Maschinenbefehle wirken sich simultan auf all diese Werte aus. Damit ist bereits ein einziger Quantenprozessor intrinsisch massiv parallel, ohne parallelisierte Hardware wie mehrere Prozessorkerne zu benötigen.

Nutzung dieser Parallelität erfordert allerdings Umgang mit dem probabilistischen Charakter der Quantenphysik und das Kompilieren von Algorithmen in quantenmechanisch erlaubte Gatter (Quantenschaltkreise). Aus diesem Grund erfordert die Nutzung der Quantenbeschleunigung zunächst die Entdeckung geeigneter Algorithmen. Zu diesen gehören bisher die schnelle Datenbanksuche, das Durchsuchen von Graphen, die Lösung linearer Gleichungssysteme, Anwendungen der schnellen Fouriertransformation einschließlich Faktorisierung und Berechnung diskreter Logarithmen, und die Simulation von Quantensystemen einschließlich Chemikalien und neuer Materialien, sowie Maschinenlernen und Optimierung. Für einige dieser Anwendungen, insbesondere die letztgenannten, ist die Quantifizierung der erreichbaren Quantenbeschleunigung noch Gegenstand aktueller Forschung. Quantencomputer sind darum – aufgrund der möglichen Anwendungen aber auch aufgrund der aufwändigen Hardware, auf der Ebene von Rechenzentrumstechnologie und Höchstleistungsrechnen anzusiedeln und keine Büro- oder gar mobile Technologie.

Quantencomputer wurden zunächst als hypothetische, theoretische Konstruktion eingeführt. Inzwischen, nach mehr als 20 Jahren Entwicklung seit den ersten Laborexperimenten, beginnt sich das Feld der Hardwareplattformen zu konsolidieren und Zugriff auf Quantenprozessoren wird als Dienstleistung von mehreren Firmen angeboten, eine sehr spezielle Quantencomputerplattform wird auch kommerziell angeboten. Diese Quantenprozessoren erlauben die Entwicklung und Evaluation von Quantenalgorithmen, sind aber noch in keiner Anwendung klassischen Rechnern überlegen. Führende Entwickler rechnen aber damit, dass dieser als Quantum Supremacy bezeichnete Schnittpunkt in wenigen Jahren erreicht wird.

1.2 Die Relevanz von Quantencomputern für die Kryptoanalyse

Ein Großteil der heute auf breiter Basis eingesetzten asymmetrischen kryptographischen Verfahren kann nicht mehr als sicher betrachtet werden, sobald die Faktorisierung großer Ganzzahlen und die Berechnung sogenannter diskreter Logarithmen effizient möglich ist. Diese einfache Beobachtung erklärt direkt das signifikante Interesse an Quantencomputern in der kryptoanalytischen Forschung — Peter Shor zeigte erstmals, dass beide Probleme asymptotisch effizient gelöst werden können, wenn ein hinreichend großer und verlässlicher Quantencomputer verfügbar ist. Die Effizienz der Shorschen Algorithmen beruht unter anderem auf der geschickten Nutzung von Überlagerung, einer Technik die mit klassischen Bits nicht realisierbar ist. Quantencomputer verwenden als elementare Einheit Qubits, bei denen den klassischen Werten 0 und 1 lediglich die Rolle von Basiswerten zukommt, und der Wert eines Qubits komplex gewichtete Anteile beider Basiswerte simultan innehaben kann. In ähnlicher Weise werden klassische Bitregister durch komplexe Quantenregister ersetzt, die effiziente hochdimensionale Berechnungen ermöglichen. Aus praktischer Sicht stellt sich die Frage, wie groß ein Quantencomputer sein muss, um real eingesetzte kryptographische Verfahren, etwas aus der RSA-Familie oder aus der Elliptischen-Kurven-Kryptographie, zu gefährden. Hierzu ist eine genauere Analyse bekannter Quantenalgorithmen erforderlich. Die abstrakten Schritte eines Quantenalgorithmus müssen für das konkret angegriffene Verfahren (effizient) in Elementarschritte umgesetzt werden, die wiederum auf reale Hardware abbildbar sind.

Detaillierte Kostenanalysen sind erst in geringem Umfang in der Literatur verfügbar, und es ist realistisch anzunehmen, dass die bislang veröffentlichten Quantenschaltkreise noch weiter optimiert werden können. Aber die verfügbaren Arbeiten lassen es bereits machbar erscheinen, die Shorschen Algorithmen für kryptographisch interessante Parameterwahlen in Quantenschaltkreise moderater Komplexität zu übersetzen.
Konkret werden für einen Angriff auf 2048 Bit RSA insgesamt $5.5 \cdot 10^{15}$ Elementarschritte auf 4098 logischen Qubits benötigt, für den diskreten Logarithmus auf einer elliptischen Kurve über 256 Bit werden 10^{14} Rechenschritte auf 2330 logischen Qubits benötigt. Dies sollte nicht mit den physikalischen Qubits verwechselt werden, deren Zahl wir in Abschnitt 1.5 angeben.
Für die symmetrische Kryptographie bieten Quantencomputer ebenfalls neue kryptoanalytische Möglichkeiten, aber mit den momentan bekannten Algorithmen sind die Auswirkungen deutlich weniger spektakulär als im asymmetrischen Fall. Auch hier kann davon ausgegangen werden, dass die besten vorhandenen quantitativen Aussagen, etwa zur Schlüsselsuche bei AES-128 noch verbessert werden, aber eine Vergrößerung der Schlüssellänge erscheint momentan eine wirksame Gegenmaßnahme.
Spektakulärere Quantenangriffe auf symmetrische Primitive sind bekannt, aber gerne wird hier ein Angriffsmodell verwendet, welches bei heute genutzten Implementierungen nicht realistisch ist.

1.3 Hardware für Quantencomputer

Die gesicherten Erkenntnisse über Quantenalgorithmen wären nicht relevant, würde nicht parallel Hardware entwickelt. Es werden eine ganze Reihe von Hardwareplattformen weltweit verfolgt, die durchaus dramatisch unterschiedlich sind—etwa vergleichbar mit dem Übergang von mechanischen zu elektronischen Computern. Die augenblicklich führenden Plattformen sind

1. Gefangene Ionen—eine Plattform die u.a. mit der Technologie von Atomuhren verwandt ist.
2. Integrierte Schaltkreise aus Supraleitern—eine Plattform, die Ähnlichkeit mit aktuellen Computerchips hat, jedoch aus anderen Materialien besteht und bei sehr tiefen Temperaturen betrieben wird.

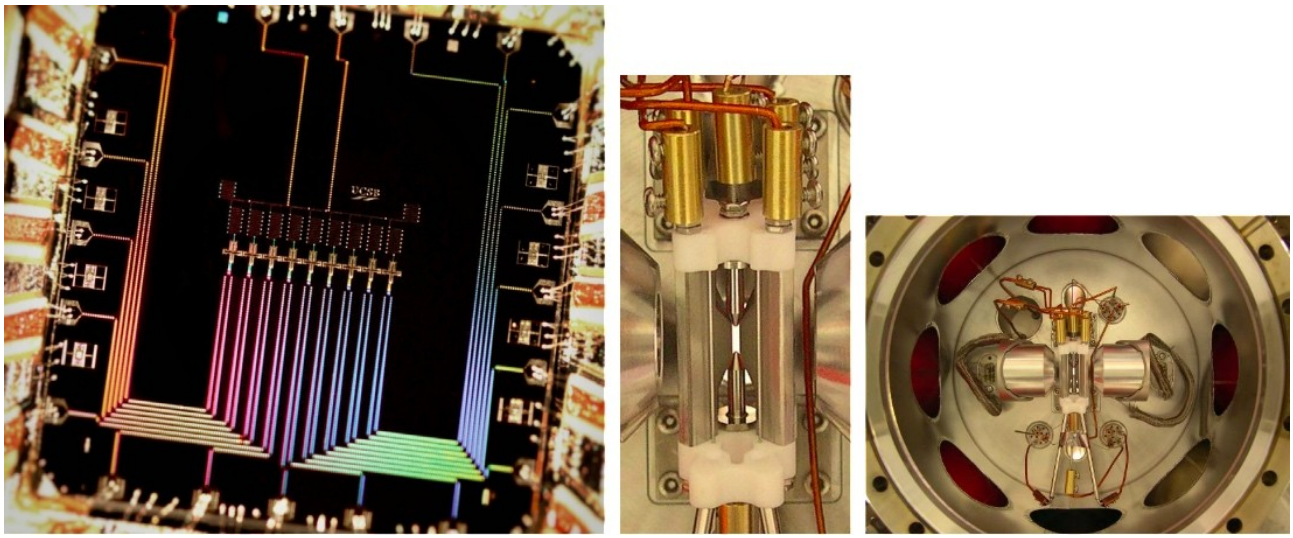

Abbildung 1: Die augenblicklich führenden Quantencomputing-Plattformen—mikroskopische Perspektive. Links: Josephson-Prozessor (Foto: Julian Kelly, Google); Mitte: Lineare Ionenfalle (Foto: Jürgen Eschner, Universität des Saarlandes); Elektroden zum Fangen (Stäbe) und Linsen zum Einstrahlen von Lasern für Quantenlogik (links und rechts); Rechts: Die gleiche Ionenfalle eingebettet in ihre Vakuumapparatur.

Es wird eine Vielzahl weiterer Plattformen erforscht, die im Augenblick weniger weit fortgeschritten sind, darunter Nanostrukturen in Halbleitern, gezielt dotierte künstliche Diamanten und Atome in Laserfeldern. Es ist durchaus möglich, dass diese Plattformen in den kommenden Jahren aufholen. Die führenden Plattformen erleben gerade den Übergang von naturwissenschaftlicher Grundlagenforschung in angewandte Forschung unter Industriebeteiligung und inhaltlich den Übergang von grundlegenden

wissenschaftlichen zu technologischen Herausforderungen bei der Entwicklung komplexer, gesteuerter Quantensysteme.
Die strukturelle Herausforderung des Gebietes ist dabei die Fehleranfälligkeit von Quantencomputern. Diese geht über das Technologische hinaus und ist grundsätzlicher Natur—der besondere Glücksfall der Fehlertoleranz von klassischen Digitalrechnern tritt hier nicht ein. Quantencomputer können kryptoanalytische Aufgaben realistisch nur dann bewältigen, wenn sie aktiv fehlerkorrigiert werden. Ein konsistentes theoretisches Gerüst dieser Fehlerkorrektur wurde entwickelt. Seine praktische Umsetzung ist Gegenstand intensiver Forschung und erste Erfolge wurden erzielt. Diese Fehlerkorrektur beeinträchtigt die grundsätzliche Effizienz von Quantencomputing nicht, ist aber trotzdem durch einen enormen Overhead gekennzeichnet—die *logischen* Quantenbits (Qubits) die einen Algorithmus beschreiben bestehen aus einer großen Zahl von Bauelementen, die *physikalische* Qubits darstellen. Auch bei großem Fortschritt ist davon auszugehen, dass der Bau eines leistungsfähigen fehlertoleranten Quantencomputers nicht nur eine wissenschaftlich-technische Herausforderung darstellt, sondern im Ergebnis eine Großanlage vom Umfang eines Rechenzentrums wäre.

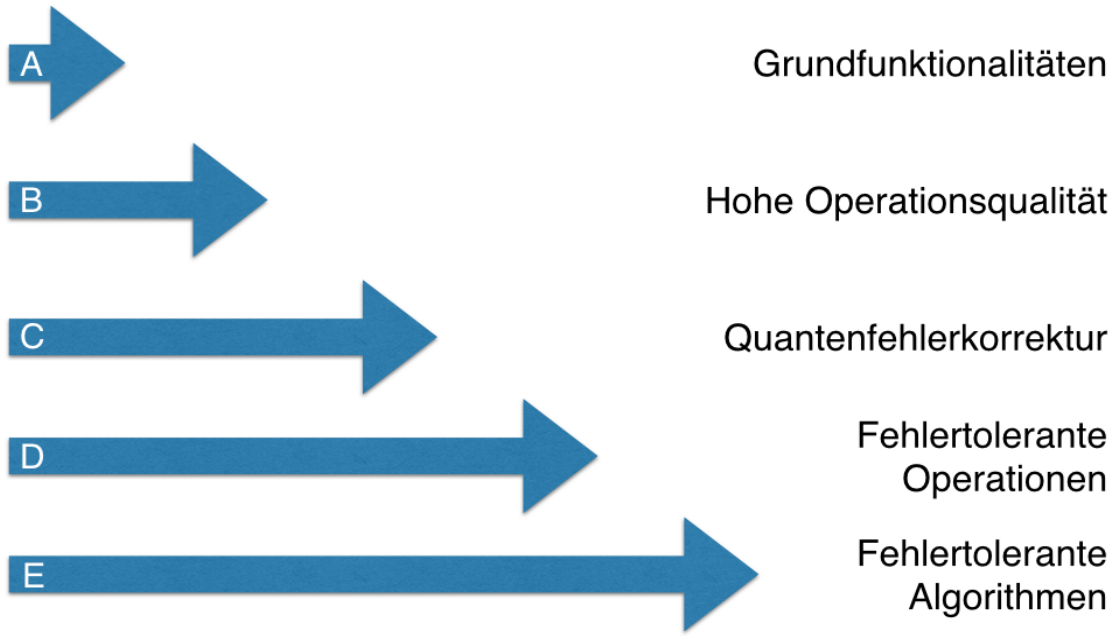

Abbildung 2: Schichtenmodell zur Bewertung von Quantencomputerplattformen anhand demonstrierter Schritte zur Fehlertoleranz

Forschungsergebnisse und die sie begleitenden Schlagzeilen können im Kontext der benötigten aktiven Fehlerkorrektur evaluiert werden. Die Studie enthält darum ein Schichtenmodell zur Bewertung von Quantencomputer-Kandidaten, beginnend mit der Demonstration von Grundfunktionen (Schicht A) bis hin zur fehlertoleranten Implementierung von Algorithmen (Schicht E), Abbildung 2. Augenblicklich wird von den führenden Plattformen Schicht C erreicht. Das Feld an Plattformen ist dicht und schnelle Veränderung der Bewertung wird erwartet, Abbildung 3.

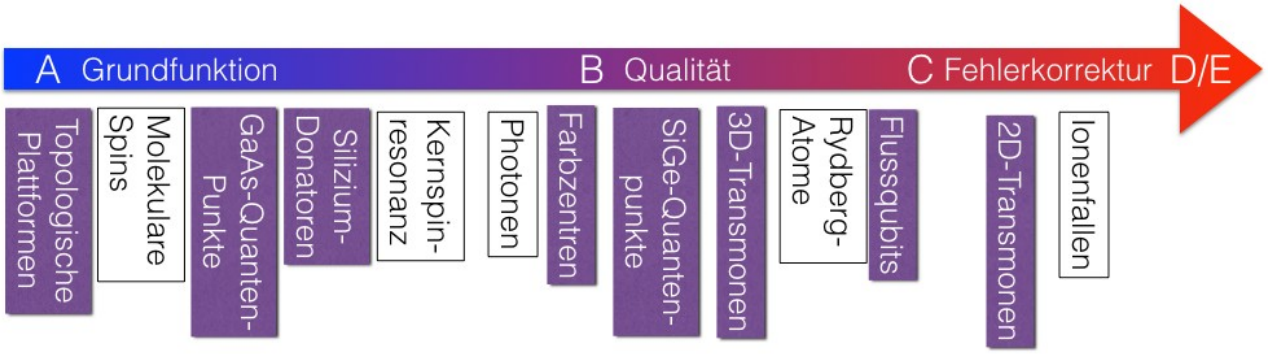

Abbildung 3: Einordnung verschiedener Plattformen im Schichtenmodell. Atomphysikalisch/optische Systeme sind weiß und Festkörpersysteme lila hinterlegt.

1.4 Aktuelle Entwicklungen

Quantencomputer und ihre Anwendungen sind augenblicklich fast wöchentlich in den Schlagzeilen der Technikpresse. Insbesondere wird dort ein „Rennen“ zur Realisierung von Quantencomputern mit den Hauptakteuren Google, IBM und—in etwas anderen Rollen—D-Wave Systems aus Kanada sowie Microsoft beschrieben. Dies spiegelt die reale rasante Entwicklung des Gebietes—auch während dieser Studie—wider. Die dort beschriebenen Systeme enthalten 20–50 *physikalische* Qubits, deren Qualität bei weitem nicht ausreicht, Kryptoanalyse ohne Fehlerkorrektur zu erreichen. Ihr Interesse liegt in einem eingeschränkten Bereich von nicht-kryptographischen Anwendungen von Quantencomputern z.B. in der Quantensimulation.
Unsere Studie schätzt, dass bei robustem technologischem Fortschritt (entsprechend einer Fehlerrate von 1:10000) zum Brechen von 2048-bit RSA in 100 Tagen etwa eine Million physikalische Qubits, in 1 Stunde etwa eine Milliarde physikalische Qubits benötigt werden, siehe Abbildung 4c. Die unterschiedlichen Zahlen erklären sich aus einem Platz-Zeit-Kompromiss in der Quantenfehlerkorrektur. Dies liegt noch Größenordnungen über den aktuell realisierten Zahlen. Bei heutigen Fehlerraten wäre die Zahl der benötigten physikalischen Qubits hundert mal so groß, siehe Abbildung 4a und 4b. Auch mit dem Overhead der Fehlerkorrektur stellt dies eine *Schwelle* dar: Wenn Quantencomputer einmal asymmetrische Kryptographie erfolgreich angreifen können, dann ist eine weitere Vergrößerung der Schlüssel in der gleichen kryptographischen Technik nicht erfolgversprechend—der zum erfolgreichen Angriff benötigte Quantencomputer ist nur wenig größer. Dieser Zusammenhang wird verdeutlicht in Abbildung 4c. Dort ist der Zusammenhang zwischen der Größe kryptoanalytischer Aufgaben, der Fehlerrate, und der Zahl der physikalischen Qubits dargestellt. Es zeigt einerseits die Größe des zu überwindenden Weges, andererseits aber auch durch die enge Lage der Kurven dass nach dem Erreichen der untersten Kurven sehr schnell die ganze Kurvenschar erreichbar sein kann.
Es ist allerdings zu beachten, dass die aktuelle Entwicklung sich vermutlich noch beschleunigt: Nachdem im ersten Jahrzehnt der ernsthaften Hardwareforschung an Quantencomputern vor allen Dingen akademische Akteure in traditionellen Programmen aktiv waren, treten jetzt einerseits starke Industrieakteure auf den Plan, andererseits werden große Forschungsprogramme wie das EU-Quantentechnologieflaggschiff aufgelegt. Eine Sonderrolle nehmen hier die USA ein, wo Forschungsförderung von Militär und Heimatschutzministerium schon sehr lange die Erforschung und Entwicklung von Quantencomputern fördern. Da die technologischen Schritte, die für einen fehlertoleranten, kryptoanalytisch relevanten Quantencomputer relevant sind (große Zahl Qubits, geringe Fehlerrate) auch die aktuellen Herausforderungen prägen, ist jeder Fortschritt hier auch ein Schritt näher an einen kryptographisch relevanten Quantenrechner.

1.5 Extrapolation

Der große Aufwand für Fehlerkorrektur macht es auf absehbare Zeit unwahrscheinlich und vermutlich auch wirtschaftlich uninteressant für akademische und industrielle Labors, einen kryptographisch relevanten Quantencomputer zu realisieren. Wenn jedoch eine große Industrienation ihre Forschungsanstrengungen auf dieses Ziel konzentrieren würde, ähnlich den Manhattan- und Apollo-Projekten des 20. Jahrhunderts, so erscheint ein Quantencomputer mit wenigen Millionen physikalischer Qubits, der zumindest in 100 Tagen 2048-Bit RSA brechen kann, erreichbar, wenn auch die physikalische Fehlerrate angemessen sinkt und in einen Bereich von 1:10000 gebracht werden kann. Dies wäre eine Großanlage, die in mehrerlei Hinsicht technologische Rekorde benötigen würde und ggf. Zugriff auf seltene Materialien erfordert.
Die Forschung an Quantencomputern entwickelt sich sehr schnell. Für supraleitende Qubits lässt sich diese Entwicklung unterteilen in eine Entwicklungsperiode von 1999–2015 und die Ära der Cloud-Quantenprozessoren seit Frühjahr 2016. Sollte die Ankündigung von 50 bzw. 72 Qubits als nächsten Meilenstein von IBM und Google im Jahr 2018 ebenfalls eintreten, was durchaus wahrscheinlich ist, entspricht dies einer Verdreifachung jedes Jahr.
Auch im aktuellen Zeitalter erster kommerzieller Anwendungen ist die Forschung an Quantencomputern noch jung genug, dass überraschende qualitative Basisinnovationen, die zu einer Beschleunigung ihrer Entwicklung führen könnten, weiterhin möglich sind.

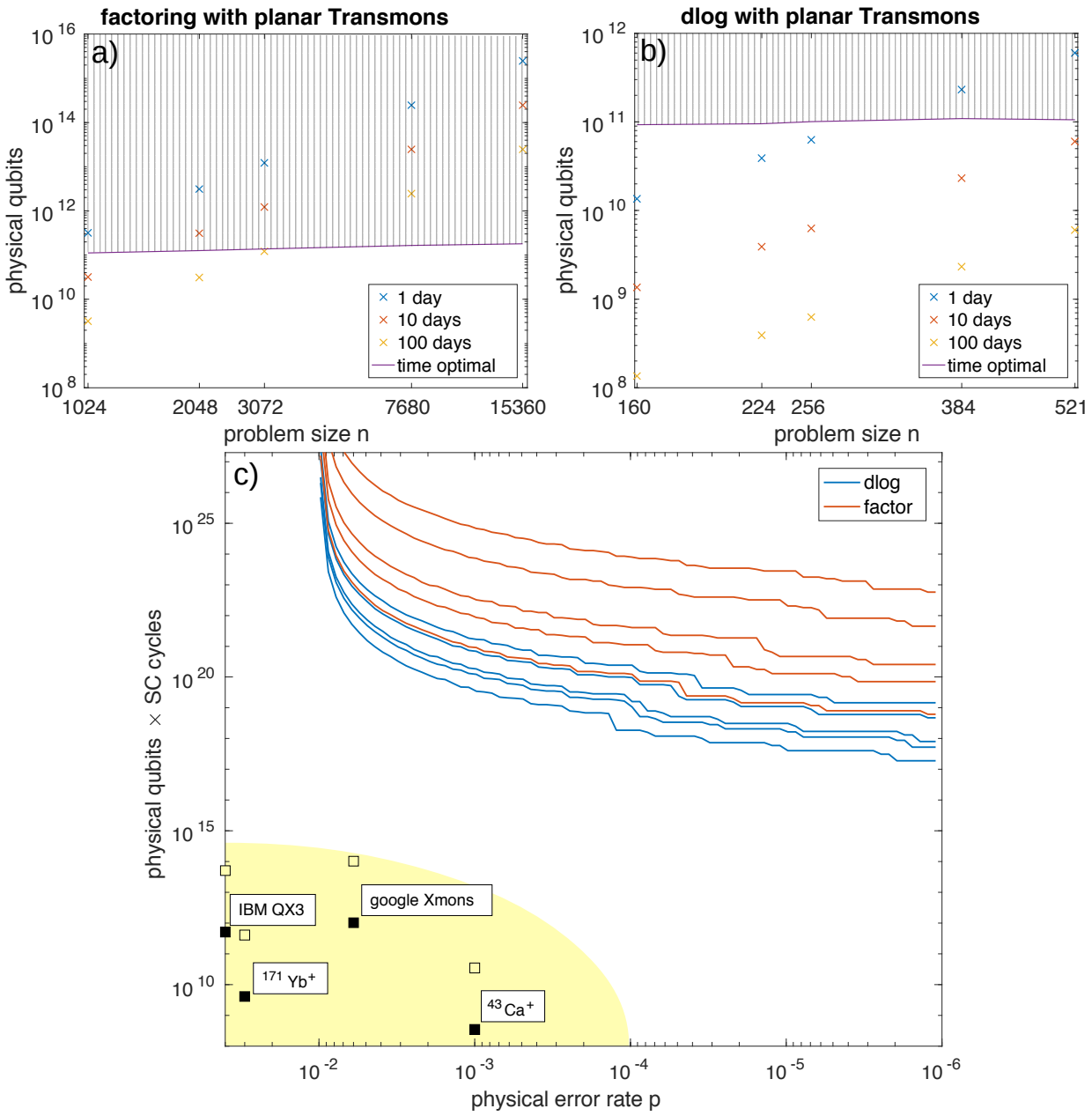

Abbildung 4: Standortbestimmung: Anforderungen an die Größe von Quantencomputern zur a) Faktorisierung und b) dem diskreten Logarithmus bei heutigen Fehlerraten für verschiedene Laufzeiten als Funktion der Problemgröße c) Wechselspiel von Fehlerrate und Zahl der Qubits für algorithmische Anwendungen. Gelber Bereich: Stand der Forschung anhand einzelner Experimente bei Laufzeit von einem Tag (gefüllt) oder 100 Tagen (offen); Linien: Anforderungen von dlog für 160,224,256,384 und 521 Bit bzw. Faktorisierung für RSA von 1024, 2048, 3072, 7680 und 15360 bit.