Quantum Computing und Bedrohung der Sicherheitstechnik

Mitsuhiro Kitajima, Martin Schider

Paris Lodron University of Salzburg

Überblick

Was ist Quantencomputer/computing?

Bedrohungen von Sicherheitstechnik

Was ist Quantencomputer/computing?

- Neue Rechnermodelle mit Quantenmechanik.
- Kann einige Probleme effizient lösen (z.B. Suchalgorithmus, Faktorisierung).
- Mögliche Anwendungen:
  - Kryptoanalyse
  - Maschinelles Lernen
  - Optimierungsprobleme (wie das Rucksackproblem)

Qubit

- Qubit ist das Bit“ in Quantencomputern.
- Jedes Qubit hat drei Zustände, basierend auf dem Superpositionsprinzip.
- Darstellung: $a|0\rangle + b|1\rangle$, wobei a und b Wahrscheinlichkeiten der Zustände sind und $|a|^2 + |b|^2 = 1$.
- Die Interpretation "gleichzeitig zwei Zustände" ist nicht ganz korrekt.

Quantenschaltungen

- Schaltungen kopieren das Ergebnis in klassische“ Bits.
- Klassischer Computer: Boolesche Algebra.
- Quantencomputer: Lineare Algebra.
- **Beispiele von Quantenschaltungen**
  - Eingabe der Schaltung ist (allgemein) 0.
  - Schaltung X: Äquivalent zur NOT-Schaltung.
  - Schaltung H: Ändert Qubit in Superposition.
  - Messung: Qubit messen und 0 oder 1 ausgeben.

Quantenalgorithmen

- **Shor-Algorithmus** (Shor, 1994):
  - Effiziente Quantenalgorithmen für Faktorisierungsverfahren.
  - Relevant für das RSA-Kryptosystem, da dessen Sicherheit auf der Annahme beruht, dass kein Faktorisierungsverfahren mit polynomieller Laufzeit existiert.
- **Grover-Algorithmus** (Grover, 1996):
  - Suchalgorithmus für unsortierte Daten.
  - Zeitkomplexität: $O(\sqrt{n})$, Raumkomplexität: $O(\log(n))$.
  - Macht Exhaustionsmethode effizienter.

Überblick

Was ist Quantencomputer/computing?

Bedrohungen von Sicherheitstechnik

Übersicht der Kryptologie

- **Kryptologie** umfasst:
  - Kryptographie (Verschlüsselung von Informationen).
  - Kryptanalyse (Analyse und Entschlüsselung).
- **Kryptographie**:
  - = krypto (geheim) + graphie (schreiben).
  - Wird seit ca. 3000 Jahren eingesetzt (z.B. im alten Ägypten).
  - Anwendungen: Passwörter, Kryptowährungen, elektronische Signaturen, Authentifizierung.

Symmetrische Verschlüsselung

- Sender und Empfänger teilen sich einen gemeinsamen öffentlichen Schlüssel.
- Angreifer versucht, den Schlüssel zu erraten.

Asymmetrische Verschlüsselung

- Sender benutzt öffentliche Schlüssel für Encryption.
- Empfänger entschlüsselt den Text mit private Schlüssel.
- Beispiel: RSA Encryption

RSA-Kryptosystem

- Entwickler: Ronald L. Rivest, Adi Shamir, Leonard Adleman.
- Asymmetrische Verschlüsselung.
- Beruht auf Primfaktorenzerlegung.
- Noch kein Algorithmus bekannt, der die Verschlüsselung effizient lösen kann.

Bedrohung durch Quantencomputer

- Bereits heute möglich, verschlüsselten Datenverkehr abzufangen und zu speichern.
- Mit zukünftigen Quantencomputern möglicherweise entschlüsselbar.
- **Grover-Algorithmus** für symmetrische Verschlüsselung.
- **Shor-Algorithmus** für asymmetrische Verschlüsselung.

Post-Quanten-Kryptographie

- Entwicklung neuer Algorithmen, die auch für Quantencomputer schwer zu lösen sind.
- Auf klassischer Computerhardware anwendbar.
- Verfahren:
  - Gitterbasierte Kryptographie.
  - Multivariate Kryptographie.
  - Hashbasierte Kryptographie.
  - Codebasierte Kryptographie.
  - Isogeniebasierte Kryptographie.

Quantenkryptographie

- Kryptographieverfahren, die auf quantenmechanischen Effekten beruhen.
- Verteilung von Quantenschlüsseln.
- Erzeugung von Quanten-Zufallszahlen.

Quellen

- https://kryptografie.de/kryptografie/index.htm
- https://www.ibm.com/de-de/topics/cryptography
- https://studyflix.de/informatik/rsa-verschlusselung-1608
- https://www.computerweekly.com/de/feature/Die-Auswirkungen-von-Quantum-Computing-auf-Kryptografi
- https://www.sectigo.com/de/ressourcen/was-ist-gitterbasierte-kryptografie
- https://www.psw-group.de/blog/quantencomputing-wie-sicher-ist-die-quantenverschluess
- https://pqkdemo.de/multivariate-Kryptografie
- https://de.wikipedia.org/wiki/RSA-Kryptosystem
- https://nms.kcl.ac.uk/stefan.edelkamp/lectures/itsec/slides/rsa.pdf
- https://www.all-electronics.de/elektronik-entwicklung/das-sind-die-chancen-und-risiken-von-quantencomputern-html