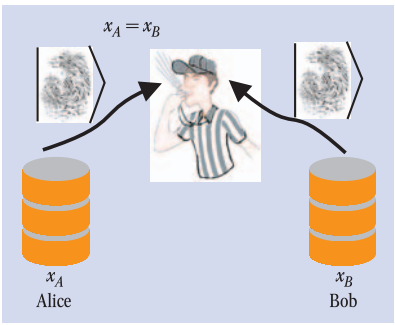
Der Quantenfingerabdruck

Der Austausch von Quantenbits erlaubt es, große Datenmengen in exponentiell kürzerer Zeit abzugleichen als mithilfe klassischer Bits.

Man stelle sich folgendes Problem vor: Alice und Bob sind Vertreter zweier Zweigstellen einer Firma und besitzen je eine große Sammlung von Daten. Die Firmenzentrale will nun überprüfen, ob die beiden Zweigstellen über genau denselben Datenbestand verfügen. Dabei dürfen die beiden Zweigstellen aber aus Sicherheitsgründen nicht direkt miteinander kommunizieren. Natürlich könnten Alice und Bob jeweils ihre gesamte Datenbank an die Zentrale übermitteln, wo Bit für Bit verglichen wird; dies ist aber bei einem großen Datenbestand ziemlich unpraktisch. Eine bessere Strategie besteht darin, nur einen wesentlich kürzeren „Fingerabdruck" der Datenbank an die Zentrale zu schicken. Der Fingerabdruck enthält dabei, ähnlich wie beim Menschen, die wesentliche Information zur Unterscheidung der Datenbestände. Wesentlich kürzer soll hier bedeuten, dass die Größe des Fingerabdrucks nur in der Größenordnung des Logarithmus der Größe der Datenbank liegt. Dies ist für einen „klassischen" Fingerabdruck nur möglich, falls Alice und Bob Zugriff auf eine korrelierte Zufallsquelle haben, etwa eine Zufallsliste von Nullen und Einsen, die nur ihnen bekannt ist. Wie in einer kürzlich erschienenen Arbeit von *Buhrman* et al. gezeigt wurde, kommen Alice und Bob jedoch ganz ohne Zufallsquelle aus, sofern sie Fingerabdrücke ihrer Datenbank verwenden, die aus *Quanteninformation* bestehen [1].



Alice und Bob besitzen je eine Datenbank; die Aufgabe des Schiedsrichters besteht darin, mithilfe von *Fingerabdrücken* der Datenbanken zu entscheiden, ob diese übereinstimmen. Sofern der Fingerabdruck aus Quanteninformation besteht, darf er exponentiell kleiner sein als die Datenbank selbst.

Die Verwendung von Fingerabdrücken ist ein Beispiel aus der Theorie der Kommunikations-Komplexität, die sich damit befasst, wie viel Informationsaustausch in Kommunikationsproblemen erforderlich ist [2]. Formaler gesprochen geht es um folgendes Problem: Alice und Bob besitzen je eine Zahl x_A und x_B in Binärdarstellung – etwa die Aneinanderreihung aller Nullen und Einsen der Datenbank. Wie viele Bits müssen Alice und Bob versenden, damit beide den Wert einer gegebenen Funktion $e \equiv f(x_A,x_B) \in \{0,1\}$ berechnen können?

Beim „Fingerprinting" geht es um eine Variante dieses Problems, in der Alice und Bob nicht direkt miteinander kommunizieren, sondern eine dritte Partei, der Schiedsrichter (*referee*), den Funktionswert berechnet (siehe Abb.). Die Funktion, um die es in diesem Beispiel geht, ist die Gleichheitsfunktion $Eq(x_A,x_B)$, die für $x_A = x_B$ den Wert Eins annimmt, ansonsten den Wert Null. Darüber hinaus verlangt man (im Rahmen eines probabilistischen Protokolls), dass der Schiedsrichter auch für die ungünstigsten Werte von x_A und x_B höchstens mit einer bestimmten Wahrscheinlichkeit die falsche Antwort gibt. Durch wenige Wiederholungen des Protokolls soll dennoch mit beliebig großer Wahrscheinlichkeit das richtige Ergebnis herauskommen.

Unter diesen Voraussetzungen gibt es keine Möglichkeit, einen wirklich kurzen Fingerabdruck zu konstruieren, der aus klassischer Information besteht – außer Alice und Bob besitzen eine korrelierte Zufallsquelle. Doch auch diese klassische Möglichkeit ist mühselig, da Alice und Bob vor jedem Datenabgleich mit einer Liste von Zufallszahlen versorgt werden müssen.

Man kann nun die Frage stellen, ob die Quanteninformatik in solchen Kommunikationsszenarien, ähnlich wie in Quantenalgorithmen beim Quantencomputer, von Vorteil ist. Zum Beispiel erlaubt die Quantenmechanik, dass Alice und Bob verschränkte EPR-Paare für die Kommunikation verwenden, etwa quantenmechanisch verschränkte Photonenpaare. Darüber hinaus ist auch der direkte Austausch von Qubits anstelle von klassischen Bits möglich. Allerdings ist seit langem bekannt, dass man mit einem Qubit maximal ein klassisches Bit übertragen kann bzw. zwei Bit, falls dieses Qubit Teil eines EPR-Paares darstellt [3], sodass sich die Frage stellt, ob man überhaupt einen darüber hinaus gehenden Vorteil, oder gar einen exponentiellen Zeitgewinn, aus der Quantenkommunikation ziehen kann.

Der Quantenfingerabdruck bildet den vorläufigen Höhepunkt einer Reihe von Arbeiten [4], die genau diese Frage mit „ja" beantworten: Erstens gilt die exponentielle Verbesserung auch für probabilistische Protokolle, und zweitens handelt es sich auch nicht um ein vereinfachtes Problem, bei dem eine bestimmte Vorabsprache über die erlaubten Werte von x_A und x_B getroffen wird (*promise problem*).

Das Quantenfingerabdruck-Protokoll nutzt die Tatsache aus, dass es in einem n-dimensionalen (komplexen) Hilbert-Raum H nicht nur n orthogonale Basisvektoren gibt, sondern auch 2^n „beinahe paarweise orthogonale" Vektoren $|h_0\rangle$, …, $|h_{2^n-1}\rangle$, d. h. für alle $i \neq j \in \{0,\ldots,2^n-1\}$ gilt: $|\langle h_i|h_j\rangle|^2 < \delta$ für ein $0 < \delta < 1$, das nicht von n abhängt. Wenn nun die Größe der Datenbank von Alice und Bob je n Bit ist, kann man die aneinandergereihten Daten als binäre Zahlen x_A und x_B zwischen 0 und 2^n-1 schreiben. Statt jedoch die großen Zahlen x_A und x_B an die Firmenzentrale zu übermitteln, senden Alice und Bob den Quantenzustand $|h_{x_A}\rangle$ bzw. $|h_{x_B}\rangle$, der in nur $\log_2 n$ Qubits kodiert werden kann. Der Schiedsrichter in der Firmenzentrale kann nun mittels elementarer Quantenrechenoperationen die Gleichheit von x_A und x_B überprüfen. Im Fall $x_A = x_B$ liefern diese mit Sicherheit das Ergebnis „1", im Fall $x_A \neq x_B$ dagegen mit der Wahrscheinlichkeit $p > (1-\delta)/2$ das Ergebnis „0".

Der Quantenfingerabdruck liefert neben der Quantenkryptographie, der Teleportation und dem Quantencomputer ein weiteres Beispiel für faszinierende Anwendungen der Quantenmechanik in der Kommunikation und der Informationsverarbeitung. Die Quantenmechanik erlaubt uns nicht nur, sicher zu kommunizieren, sondern in bestimmten Fällen auch wesentlich effizienter, als dies mit klassischer Kommunikation möglich ist.

Hans Aschauer und
Hans J. Briegel

[1] *H. Buhrman, R. Cleve, J. Watrous, Ronald de Wolf*, Phys. Rev. Lett. **57**, 167902 (2001).
[2] *A. C.-C. Yao*, Some Complexity Questions Related to Distributive Computing (Preliminary Report). In: ACM Symposium on Theory of Computing, Seiten 209–213 (1979).
[3] *A. Zeilinger, H. Weinfurter*, Phys. Bl., März 1996, S. 219.
[4] *G. Brassard*, www.arXiv.org, quant-ph/0101005 (2001).

Dipl.-Phys. Hans Aschauer und Dr. Hans J. Briegel, Theoretische Physik, Ludwig-Maximilians-Universität, Theresienstr. 37, 80333 München