Kuantum Bilgisayarlar ve Kriptoloji

0, 1 veya hem 0 hem 1?

BILYAL MUSATAFA YARMADZHA
Bilgisayar Mühendisliği Bölümü, 3. sınıf

21 Mart 2024

İçindekiler

Arkaplan

Kuantum Latince '**quantus**' (ne kadar, ne büyüklükte) sözcüğünden gelir.

Kuantum bilgisayar ise kuantum mekaniği yasalarına dayalı hesaplamalar yapar, bu da atom altı seviyedeki parçacıkların davranışlarıdır.

Kuantum mekaniği kurallarına dayanarak bilgi işleme ve iletişim fikrini Richard **Feynman** ortaya atmıştır (1982).

Kaynak: Alice & Bob

Kuantum bit (kübit/qubit)

Klasik bilgisayardaki bit’i yukarı aşağı işaret eden bir ok ile gösterelim

Kaynak: Alice & Bob

O zaman bir kübiti, kürenin yüzeyindeki kutuplarında 0 ve 1 bulunan sonsuz noktalardan **herhangi birine** işaret eden bir okla temsil edebiliriz.

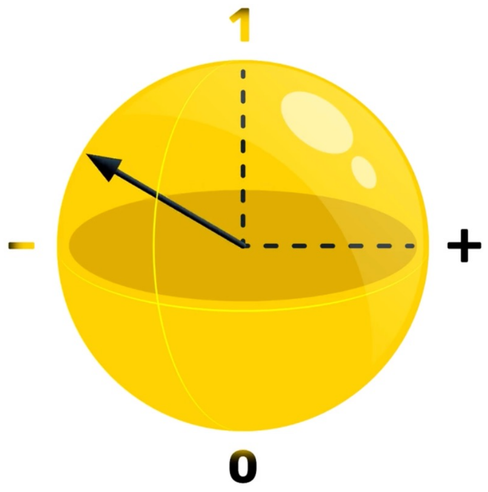
Kaynak: Alice & Bob

Süper Pozisyon

Kübit, bir bitten farklı olarak şu ya da bu durumda değildir, **ölçülene kadar** durumların **süper pozisyonundadır**.

Ölçüldüğünde ayrı bir değer (1 veya 0) verecektir, ancak ölçülene kadar durumlardan birçoğunda aynı anda bulunabilir (süper pozisyon).

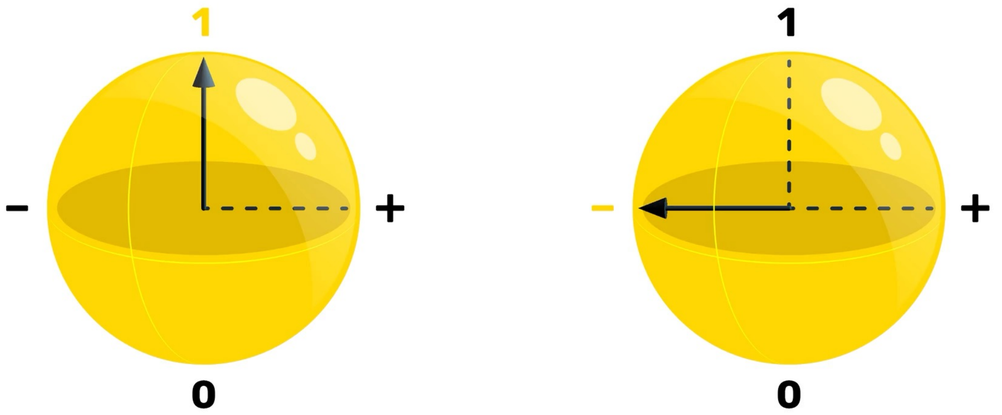
Bu nedenle kübit genellikle Bloch küresi adı verilen küreyle temsil edilir.



Bloch Küresi

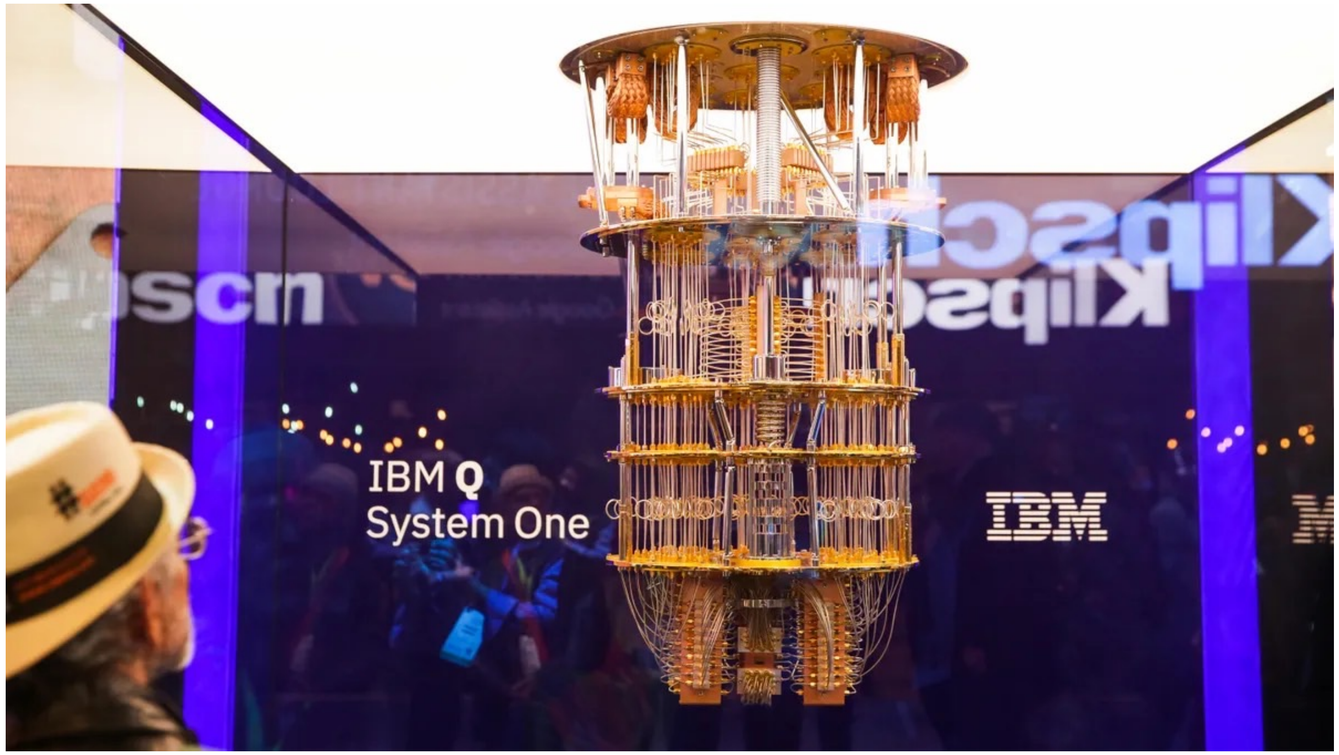
Tutarsızlık (decoherence)

- **Kübitler son derece kırılgandır.**
- Çevrelerindeki ***dış 'gürültü'*** ile hemen hemen her etkileşimleri, onların bir sufle gibi çökmesine ve **tutarsızlık** olarak bilinen yıkıcı bir süreçte kuantum bilgilerinin değişmesine veya kuantum doğalarını kaybetmelerine neden olabilir.



IBM Kuantum Bilgisayar

IBM Q dış görünüşü



IBM Q iç görüntüsü

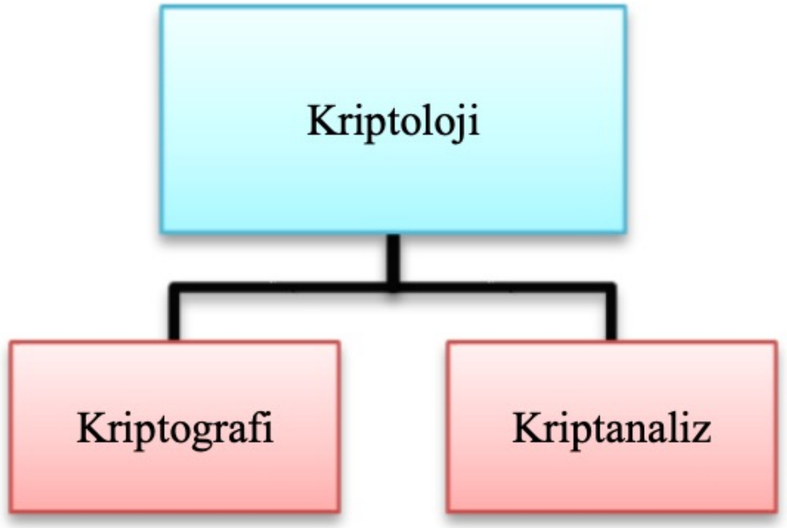
Genel olarak **n** kübit sahibi bir kuantum bilgisayarı aynı anda 2^n çakışmanın herhangi birinde olabilir. (Normal bilgisayarlar durumun sadece birinde olurken, bir kuantum bilgisayarı bu durumların hepsinde ya da bir kısmında bulunabilir. (süper pozisyon))

Kriptoloji

Kriptoloji (cryptology) aslen Yunanca olan *kryptós*: gizli, gizlenmiş ve *logia*: çalışma, inceleme, araştırma sözcüklerinin yan yana gelmesinden oluşmaktadır.

Bu bilim matematiğin alt dalı olup iki kısımdan oluşmaktadır:

- **kriptografi** - bilgiyi gizli tutma sanatı ve bilimi
- **kriptanaliz** - şifreleme yöntemlerini kıran bilim



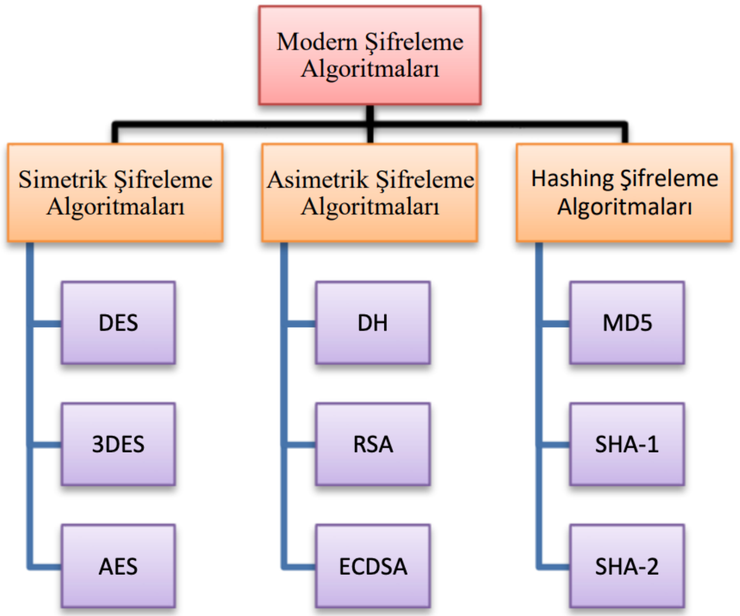
Kuantum Kriptolojisi ve Siber Güvenlik [1]

Modern Kriptoloji Yöntemleri

Bilgi güvenliğini sağlamak için **simetrik**, **asimetrik** ve **Hashing** şifreleme algoritmaları kullanılmaktadır.

Bu teknikler matematikseldir ve genellikle sayılarla yapılan büyük işlemlerden sonra çıktıyı üretirler.

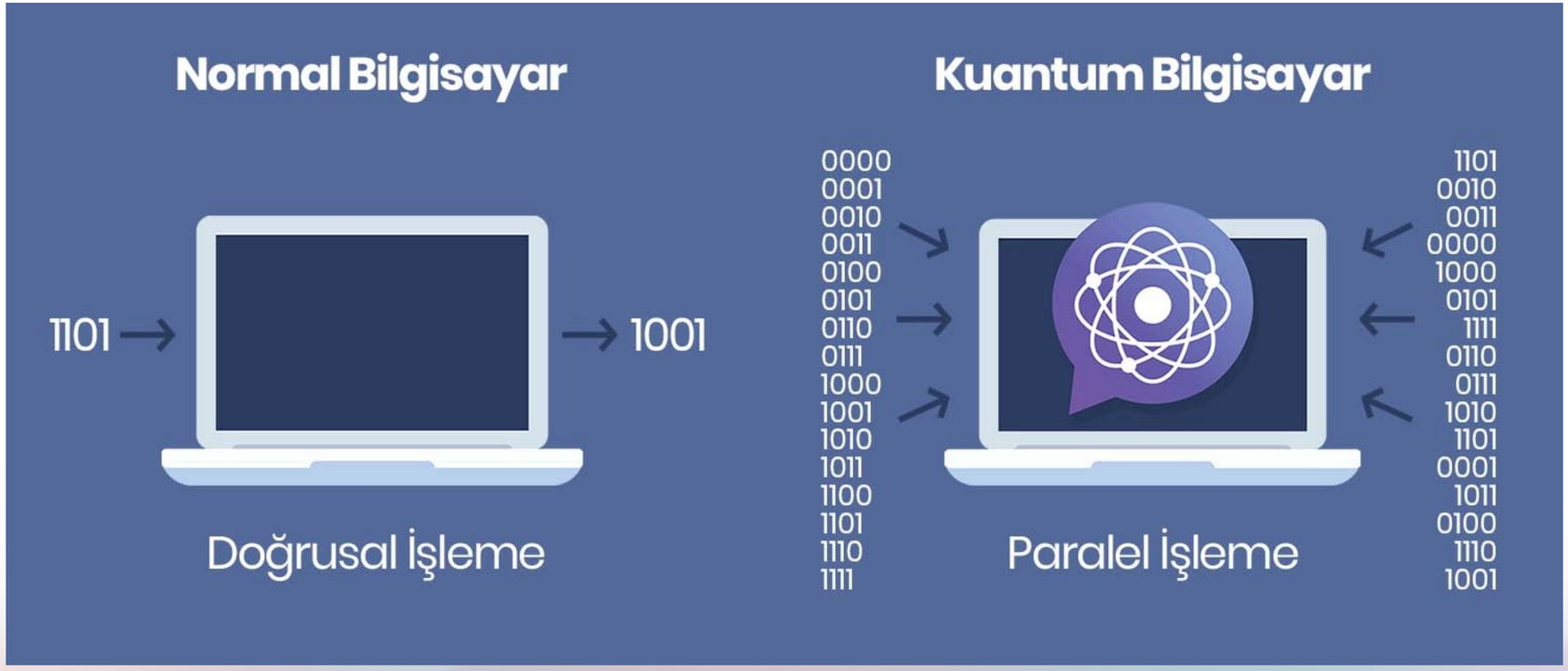
Bu matematiksel şifrelemelerin ideali ve tehlikesiz kabul edilenler klasik bilgisayarlar tarafından çözülmesi çok fazla zaman alacağı hesaplanan türdendir (10.000 yıl vb.).



Kuantum Kriptolojisi ve Siber Güvenlik [1]

Kuantum Kriptanaliz

Kuantum kriptanalizin şu an için en çok bilinen örneklerinden birisi 1994 yılında matematikçi Peter Shor tarafından önerilen **Shor** algoritmasıdır.
Shor, bir kuantum bilgisayarın inanılmaz hızlı bir şekilde çok büyük bir tamsayının asal çarpanlarına nasıl ayrılabileceğini göstermiştir.



Kuantum Kriptografi

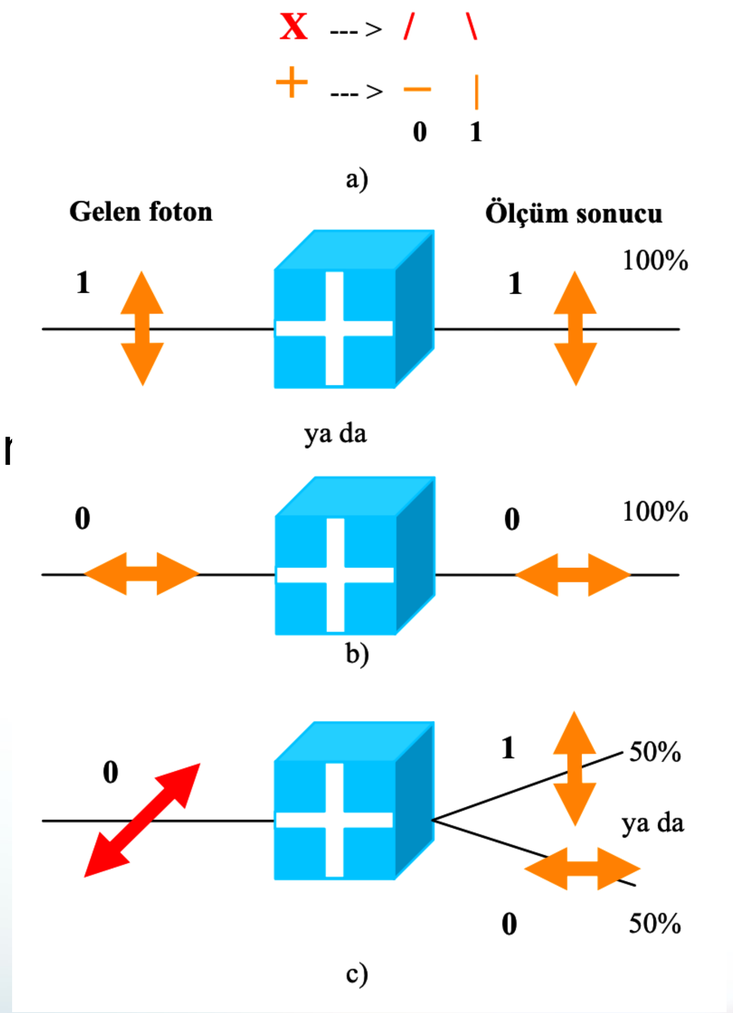
Mevcut kuantum kriptografi, şimdilik klasik ve kuantum kısımlardan oluşmaktadır:

- *kuantum kısım:* kuantum anahtar dağıtımı (KAD)
- *klasik kısım:* geleneksel kriptografi ile şifreleme

Kuantum kısmında KAD protokolleri, birbirinden çok uzakta olan iki kullanıcı arasında **aynı**, **rasgele** ve **güvenli** bir **gizli anahtar** oluşturulmasını sağlar.

KAD'ın, temel çalışma ilkesi ise şu şekildedir:

- *Anahtar*, tam *güvenli* bir şekilde dağıtılır.
- Aksi halde, protokol *iptal* edilir ve *tekrar* denenir.



Kaynakça

- Gümüş, E. (2011). Kuantum kriptografi ve anahtar dağıtım protokolleri. *Akademik Bilişim*.
- Easttom, C. (Year of Publication). Modern Cryptography: Applied Mathematics for Encryption and Information Security (2nd ed.). Publisher.
- Toyran, M., Pedersen, T. B., Hasekioğlu, A. A., Can, M. A., & Berber, S. (2011). Bilgi güvenliğinde kuantum teknikler. *BİLDİRİLER KİTABI*, 98.
- Çelik, S. (2021). Kuantum Kriptolojisi ve Siber Güvenlik. *Bilişim Teknolojileri Dergisi*, 14(1), 53. https://doi.org/10.17671/gazibtd.733309
- Şahin, M. (2014). Kuantum bilgisayarları ve bazı uygulamalar.
- Turhost, Kuantum Bilgisayar Nedir? Nasıl Çalışır?
- Alice & Bob

Sorular?

Teşekkürler!