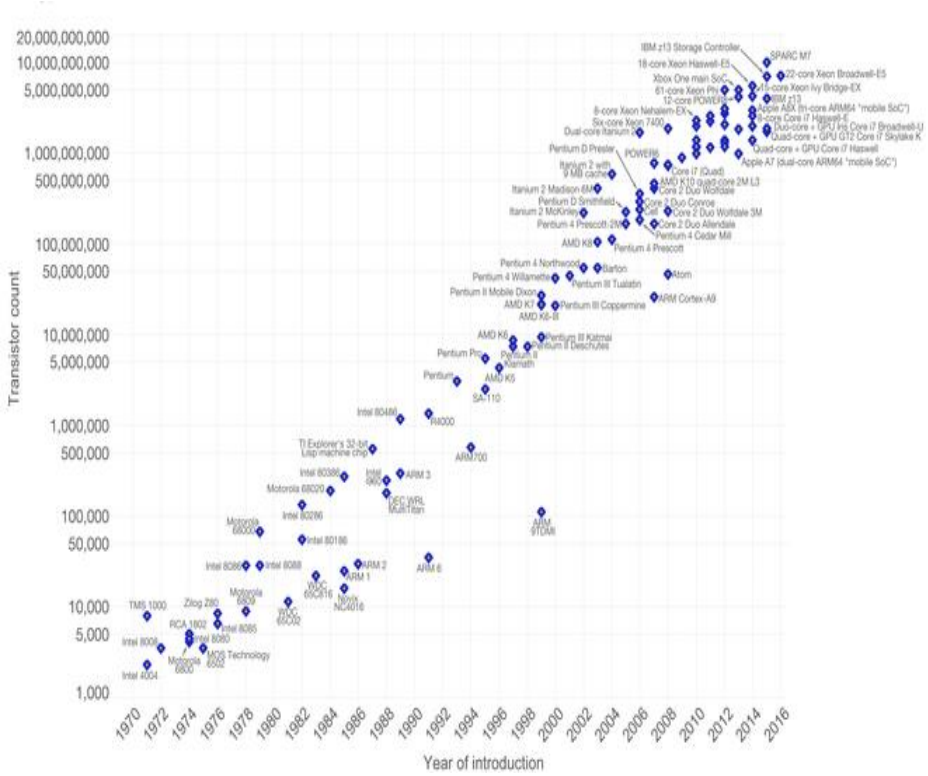
عنوان سمینار

بررسی، تحلیل و مقایسه انواع روش های توزیع کلید کوانتومی و کاربردهای آن ها

استاد راهنما : دکتر شهرام محمد نژاد

فهرست

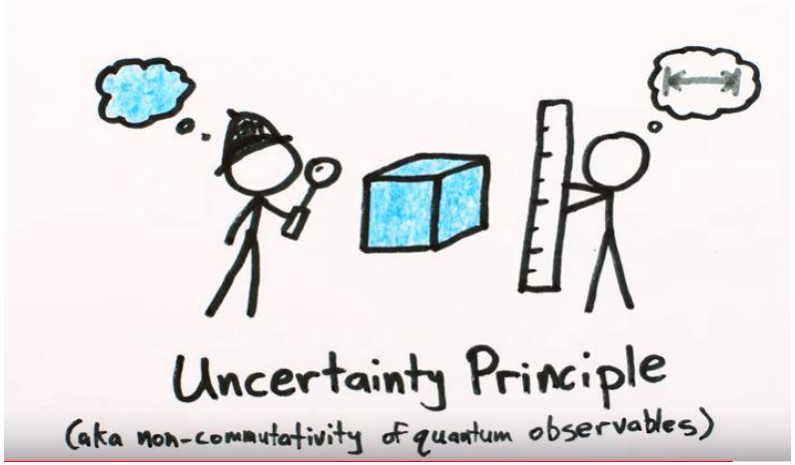
- مقدمه
  - قانون مور
  - تئوری عدم تکثیر حالت ها
- ارتباطات کوانتومی
- چالش ها در زمینه توزیع کلید کوانتومی
- انواع پروتکل ها
  - ✓ BB84
  - ✓ SARG04
  - ✓ B92
  - ✓ COW
  - Ekert91
  - EPR



قانون مور : در هر دو سال، تعداد ترانزیستور ها روی تراشه ، دو برابر می شود.

تکامل محاسباتی ⟵ **رایانه های کوانتومی**

تئوری عدم تکثیر حالت ها



اصل عدم قطعیت هایزنبرگ

هر ذره در مکانیک کوانتوم ، در سوپرپوزیشن حالت های مختلفی است.

$$|A\rangle = |A1\rangle + |A2\rangle$$

ارتباطات کوانتومی

- ✓ توزیع کلید کوانتومی
- ✓ انتقالات کوانتومی
- ✓ تکرار کننده های کوانتومی

توزیع کلید کوانتومی، بخشی از رمزنگاری کوانتومی می باشد که شامل پروتکل های مختلفی است.

چالش های انتقال کلید کوانتومی

1. نویز
2. تاخیر در انتقال فیلم ها
3. تقویت فوتون ها (نیاز به تکرار کننده های کوانتومی)
4. امنیت

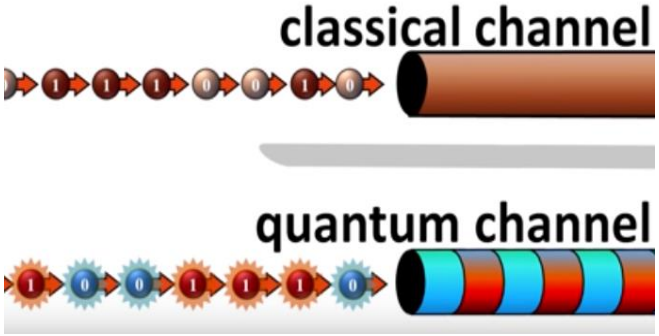
پروتکل BB84

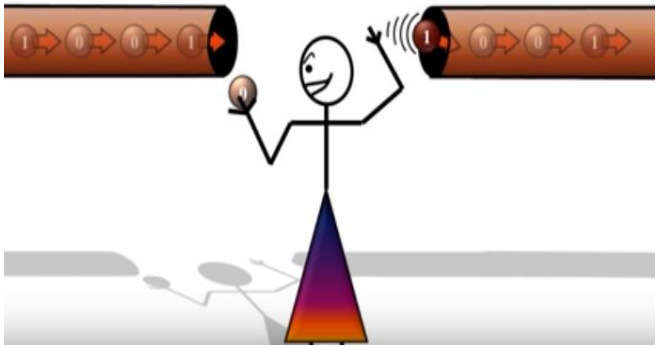
Quantum
Cryptography

Bennett Brassard ’84

انواع پروتکل ها (BB84)----------

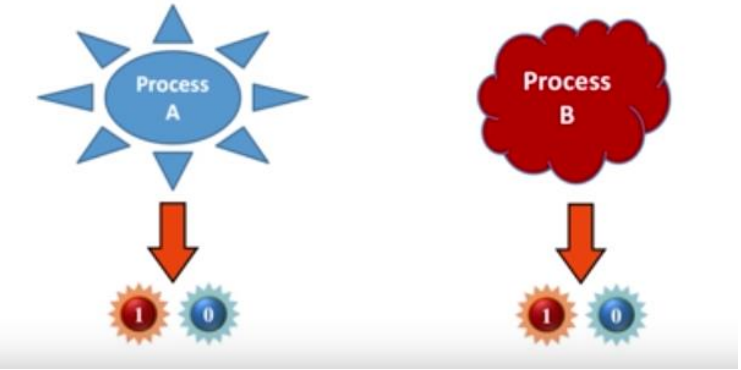
آلیس کیوبیت ها را از طریق کانال کوانتومی برای باب مبفرستد.
باب بصورت تصادفی، با یکی از روش ها، کیوبیت را اندازه گیری می کند.



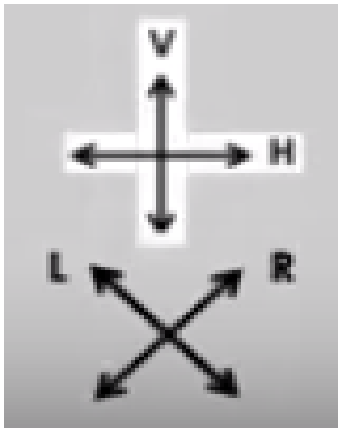


ایو، نمی تواند کیوبیت ها را کپی کند و تشخیص داده می شود.
آلیس و باب کلید امن برای رمزنگاری را به صورت اشتراکی به دست می آورند.

انواع پروتکل ها (BB84) ----------



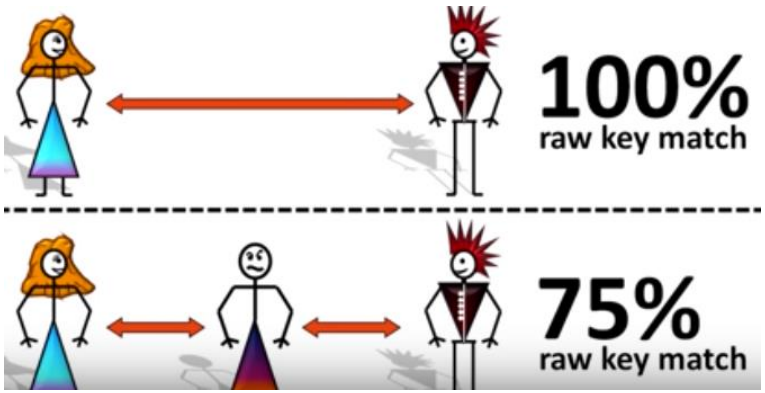
روش های اندازه گیری کیوبیت ها



قطبش افقی-عمودی

قطبش مورب

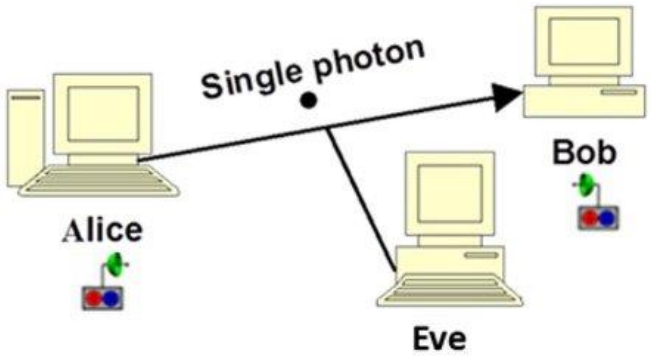
نا‌امن بودن کانال ارتباطی در صورت کاهش نرخ کلید امن



حمله PNS

منبع استفاده شده در پروتکل BB84 ، لیزر تضعیف شده، دارای بیش از یک فوتون

سرقت اطلاعات



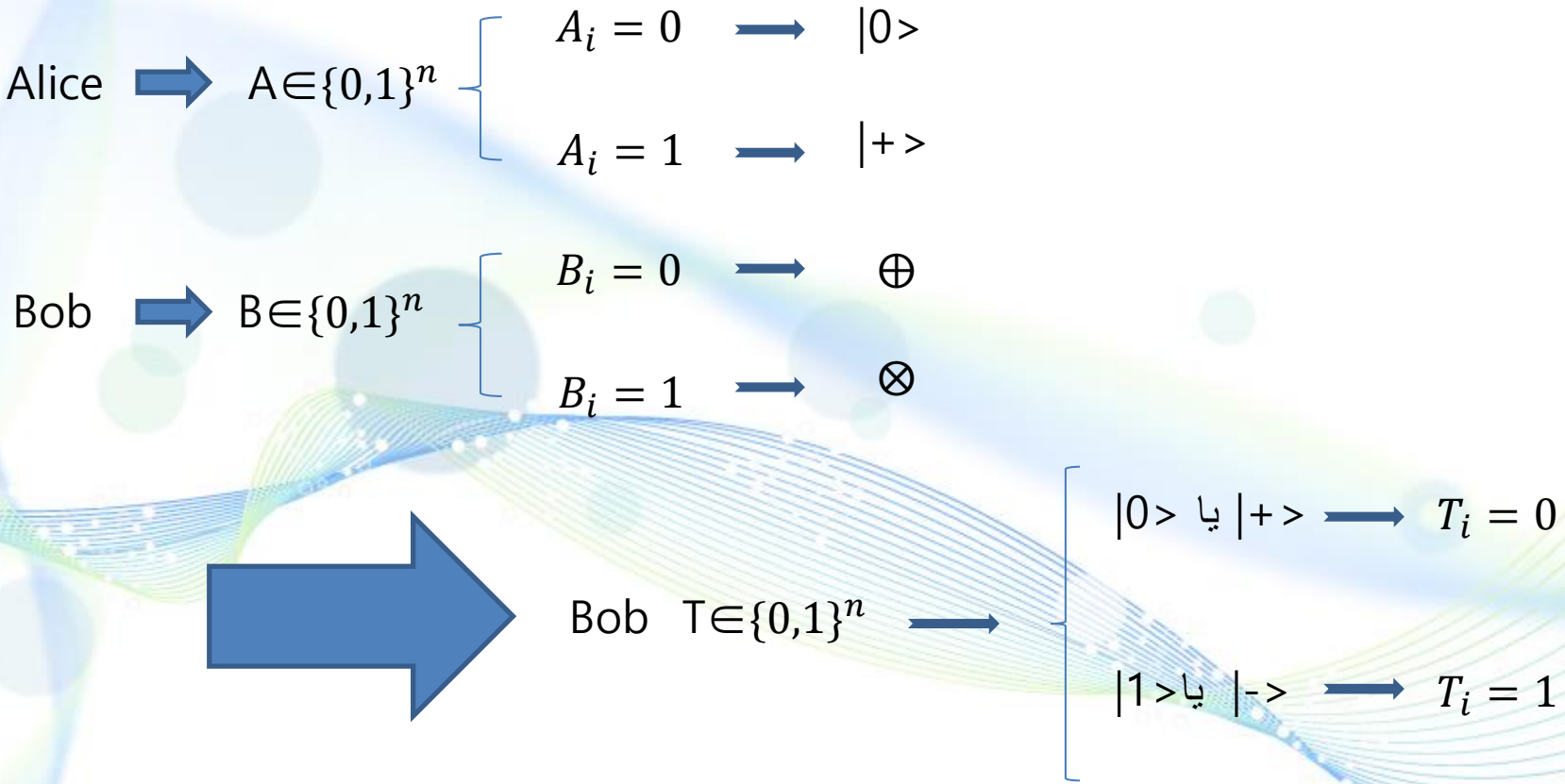
راه حل :

پروتکل SARG04

حالت های تله گذاری شده

پروتکل B92 ← ۱۹۹۲ ← Bennet

فاز اول : انتقال در کانال کوانتومی



فاز دوم : کانال کلاسیک

Alice و Bob تنها بیت هایی از بردار های A و B را که $T_i = 1$ باشد، نگه می دارند

در نتیجه داریم : $A_i = 1 - B_i$

کلید خام مشترک تشکیل می شود

Alice یک نمونه از بیت های کلید خام را از طریق کانال کلاسیکی برای Bob می فرستد

اگر i ای وجود داشته باشد که $A_i \neq 1 - B_i$ ، Eve شناسایی می شود

کلید مخفی مشترک $k \in \{0,1\}^N$ بعد از حذف نمونه های مرحله قبل با توجه به کلید خام، تشکیل می شود

پروتکل COW

- ✓ Nicolas Gisin
- ✓ 2004
- ✓ پالس های همدوس ضعیف

بر مبنای اندازه گیری زمان رسیدن خط داده

یک تداخل سنج در یک خط مانیتورینگ اضافی برای تشخیص حضور جاسوس

با تشکر از توجه شما