Quantum Cryptography

Marshall Roth
March 9, 2007

Overview

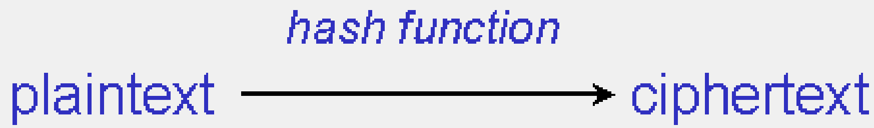
- Current Cryptography Methods
- Quantum Solutions
- Quantum Cryptography
- Commercial Implementation

Cryptography algorithms:

- *Symmetric* – encrypting and decrypting key are identical (Data Encryption Standard, Rivest Ciphers)
- *Asymmetric* – encrypting and decrypting keys differ (Elliptical Curve; Rivest, Shamir, Adleman)
- *Hash* – no decryption by design, meant to uniquely identify a message such as a password (Message Digest)

A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.



C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

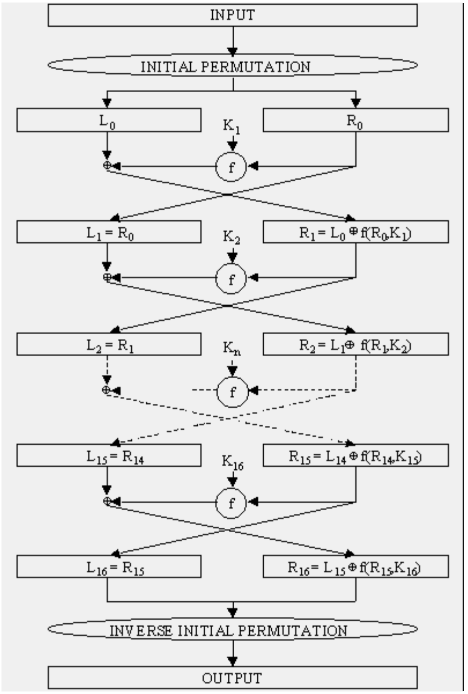
Gary Kessler 2007

Symmetric Key Distribution

- RC5 and others takes sufficiently long decrypt (72 bits with distributed computing ~1000 years for RC5)
- How do we securely distribute keys?
- Some methods work on simple binary addition:

$$s = m \oplus k, m = s \oplus k = m \oplus k \oplus k$$

- Others, such as DES, shuffle blocks of information



Asymmetric Key Distribution

- Rivest, Shamir, Adelman (RSA) use the property of factoring a large number in terms of primes is sufficiently complex with classical computers.
- Elliptical Curves make use of another sufficiently complex classical problem of calculating the discrete logarithm.
- Codes can be broken more readily than symmetric keys (72 bits sym ~ 2048 bits asym)

RSA Algorithm

- Pick two large prime numbers p and q and calculate the product $N = pq, \;\; \phi = (p-1)(q-1)$
- Choose a number that is co-prime with ϕ, c
- Find a number d to satisfy $cd = 1 \; mod \; \phi$, using a method such as Euclid's algorithm
- Using your plaintext, a, the ciphertext is encoded as $b = a^c \; mod \; N$
- To retrieve the plaintext, $a = b^d \; mod \; N$
- The numbers N and c are made public, so anyone can encrypt information, but only someone with d can retrieve the plaintext

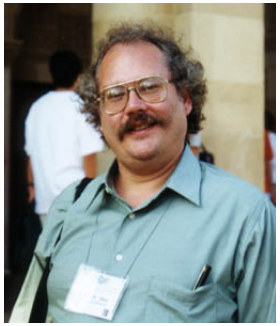
Example

- Plaintext $a = 123$
- $p = 61$ and $q = 53$
- $N = pq = 3233$
- $\phi = (p - 1)(q - 1) = 3120$
- Pick a coprime of ϕ, $c=17$
- Find d such that $cd = 1 \mod \phi$, $d=2753$
- Encode with $a^c \mod N$, in this case $123^{17} \mod 3233 = 855$
- Decode message by evaluating $b^d \mod N$, in this case $855^{2753} \mod 3233 = 123$

855^2753 mod 3233

= 50432888958416068734422899127394466631453878360035509315554967564501
05562861208255997874424542811005438349865428933638493024645144150785
17209179665478263530709963803538732650089668607477182974582295034295
04079035818459409563779385865989368838083602840132509768620766977396
67533250542826093475735137988063256482639334453092594385562429233017
51977190016924916912809150596019178760171349725439279215696701789902
13430714646897127961027718137839458696772898693423652403116932170892
69617643726521315665833158712459759803042503144006837883246101784830
71758547454725206968892599589254436670143220546954317400228550092386
36942444855973333063051607385302863219302913503745471946757776713579
54965202919790505781532871558392070303159585937493663283548602090830
63550704455658896319318011934122017826923344101330116480696334024075
04695258866987658669006224024102088466507530263953870526631933584734
81094876156227126037327597360375237388364148088948438096157757045380
08107946980066734877795883758289985132793070353355127509043994817897
90548993381217329458535447413268056981087263348285463816885048824346
58897839333466254454006619645218766694795528023088412465948239275105
77049113329025684306505229256142730389832089007051511055250618994171
23177795157979429711795475296301837843862913977877661298207389072796
76720235011399271581964273076407418989190486860748124549315795374377
12441601438765069145868196402276027766869530903951314968319097324505
45234594477256587887692693353918692354818518542420923064996406822184
49011913571088542442852112077371223831105455431265307394075927890822
60604317113339575226603445164525976316184277459043201913452893299321
61307440532227470572894812143586831978415597276496357090901215131304
15756920979851832104115596935784883366531595132734467524394087576977
78908490126915322842080949630792972471304422194243906590308142893930
29158483087368745078977086921845296741146321155667865528338164806795
45594189100695091965899085456798072392370846302553545686919235546299
57157358790622745861957217211107882865756385970941907763205097832395
71346411902500470208485604082175094910771655311765297473803176765820
58767314028891032883431850884472116442719390374041315564986995913736
51621084511374022433518599576657753969362812542539006855262454561419
25880943740212888666974410972184534221817198089911953707545542033911
96453936646179296816534265223463993674233097018353390462367769367038
05342644821735823842192515904381485247388968642443703186654199615377
91396964900303958760654915244945043600135939277133952101251928572092
59788751160195962961569027116431894637342650023631004555718003693586
05526491000090724518378668956441716490727835628100970854524135469660
84481161338780654854515176167308605108065782936524108723263667228054
00387941086434822675009077826512101372819583165313969830908873174174
74535988684298559807185192215970046508106068445595364808922494405427
66329674592308898484868435865479850511542844016462352696931799377844
30217857019197098751629654665130278009966580052178208139317232379013
23249468260920081998103768484716787498919369499791482471634506093712
56541225019537951668976018550875993133677977939527822273233375295802
63122665358948205566515289466369032083287680432390611549350954590934
06676402258670848337605369986794102620470905715674470565311124286290
73548884929899835609996360921411284977458614696040287029670701478179
49024828290748416008368045866685507604619225209434980471574526881813
18508591501948527635965034581536416565493160130613304074344579651083
80304062240278898042825189094716292266898016684480963645198090510905
79651307570379245958074479752371266761011473878742144149154813591743
92799496956415653866883891715446305611805369728343470219206348999531
11429937000557751339717282549110056008940898419671319709118165542908
76109008324997831338240786961578492341986299168008677495934077593066
02207814943807854996798945399364063685722697422361858411425048372451
24465580270859179795591086523099756519838277952945756996574245578688
38354442368572236813990212613637440821314784832035636156113462870198
51423901842909741638620232051039712184983355286308685184282634615027
44187358639504042281512399505995983653792227285847422071677836679451
34363807086579774219853595393166279988789721695963455346336497949221
13017661316207477266113107012321403713882270221723233085472679533015
07998062253835458948024820043144726191596190526034069061930939290724
10284948700167172969517703467909979440975063764929635675558007116218
27727603182921790350290486090976266285396627024392536890256337101471
68327404504583060228676314215815990079164262770005461232291921929971
69907690169025946468104141214204472402661658275680524166861473393322
65959127006456304474160852916721870070451446497932266687321463467490
41185886760836840306190695786990096521390675205019744076776510438851
51941619318479919134924388152822038464729269446084915299958818598855
19514906630731177723813226751694588259363878610724302565980914901032
78384821401136556784934102431512482864529170314100400120163648299853
25166349056053794585089424403855252455477792240104614890752745163425
13992163738356814149047932037426337301987825405699619163520193896982
54478631309773749154478427634532593998741700138163198116645377208944
00285485000269685982644562183794116702151847721909339232185087775790
95933267631141312961939849592613898790166971088102766386231676940572
95932538078643444100512138025081797622723797210352196773268441946486
16402961059899027710532570457016332613431076417700043237152474626393
99011899727845362949303636914900881060531231630009010150839331880116
68215163893104666659513782749892374556051100401647771682271626727078
37012242465512648784549235041852167426383189733332434674449039780017
84689726405462148024124125833843501704885320601475687862318094090012
63241969092252022679880113408073012216264404133887392600523096072386
15855496515800103474611979213076722454380367188325370860671331132581
99227975522771848648475326124302804177943090938992370938053652046462
55147267884961527773274119265709116613580084145421487687310394441054
79639308530896880365608504772144592172500126500717068969428154627563
70458838904219177398190648731908014828739058159462227867277418610111
02763247972904122211994117388204526335701759090678628159281519982214
57652796853892517218720090070389138562840007332258507590485348046564
54349837073287625935891427854318266587294608072389652291599021738887
95773647738726574610400822551124182720096168188828493894678810468847
31265541726209789056784581096517975300873063154649030211213352818084
76122990409576427857316364124880930949770739567588422963171158464569
84202455109029882398517953684125891446352791897307683834073696131409
74522985638668272691043357517677128894527881368623965066654089894394
95161912002160777898876864736481837825324846699168307281220310791935
64666840159148582699993374427677252275403853322196852298590851548110
40229657916338257385513314823459591633281445819843614596306024993617
53097925561238039014690665163673718859582772525683119989984646027216
46279764077057074816406450769779869955106180046471937808223250148934
07851137833251073753823403466269553292608813843895784099804170410417
77608463062862610614059615207066695243018438575031762939543026312673
77406936404705896083462601885911184367532529845888040849710922999195
65539701911119191918832730860376677533960772245563211350657219106758 7
51186812786344197572392195263333856538388240057190102564949233944519
65959203992392217400247234147190970964562108299547746193228981181286
05556588093851898811812905614274085809168765711911224763288658712755
38928438126611991937924624112632990739867854558756652453056197509891
14578114735771283607554001774268660965093305172102723066635739462334
13638045914237759965220309418558880039496755829711258361621890140359
54234930424749053693992776114261796407100127643280428706083531594582
305946326827861270203356980346143245697021484375 mod 3233

Enter Shor's Algorithm



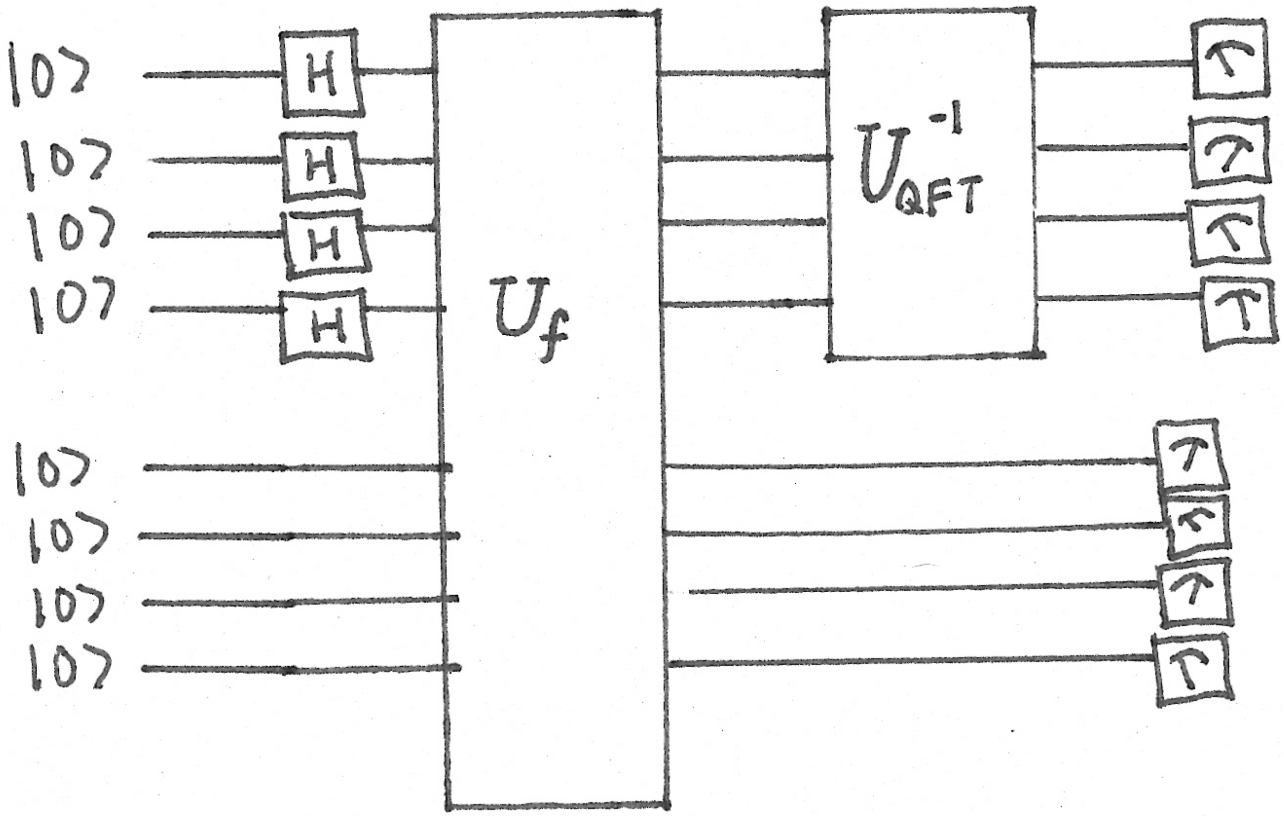
- Let $f(x) = b^x \mod N$, if we can find some r that $f(x) = f(x+r)$, then we can find a number d' such that $cd' = 1 \mod r$
- The value d' works like the decoding value we calculated from $cd = 1 \mod \phi$
- In addition, using different values for $b<N$, we can determine the prime components of N

What's the quantum algorithm?

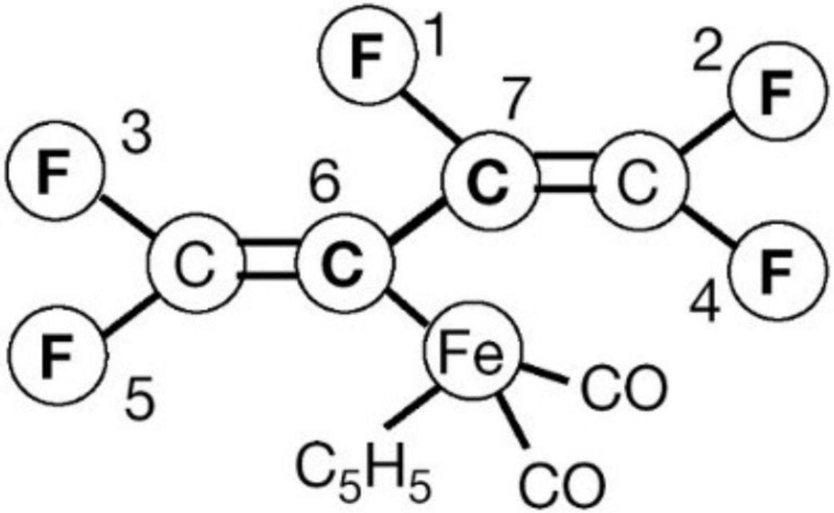
- Initialize $log_2 N$ qubits an equal superposition state (input qubits)

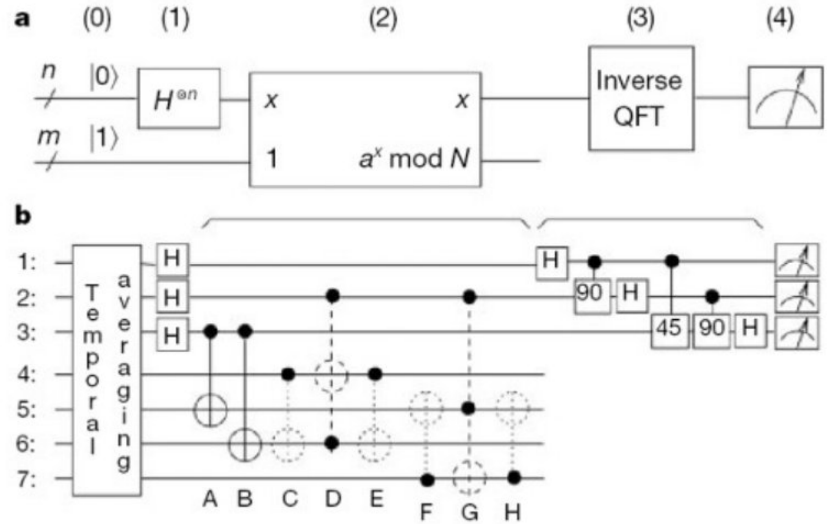
$$|\psi\rangle = \frac{1}{2^{n/2}}\left(|000...000\rangle + |000...001\rangle + ... + |111...111\rangle\right)$$

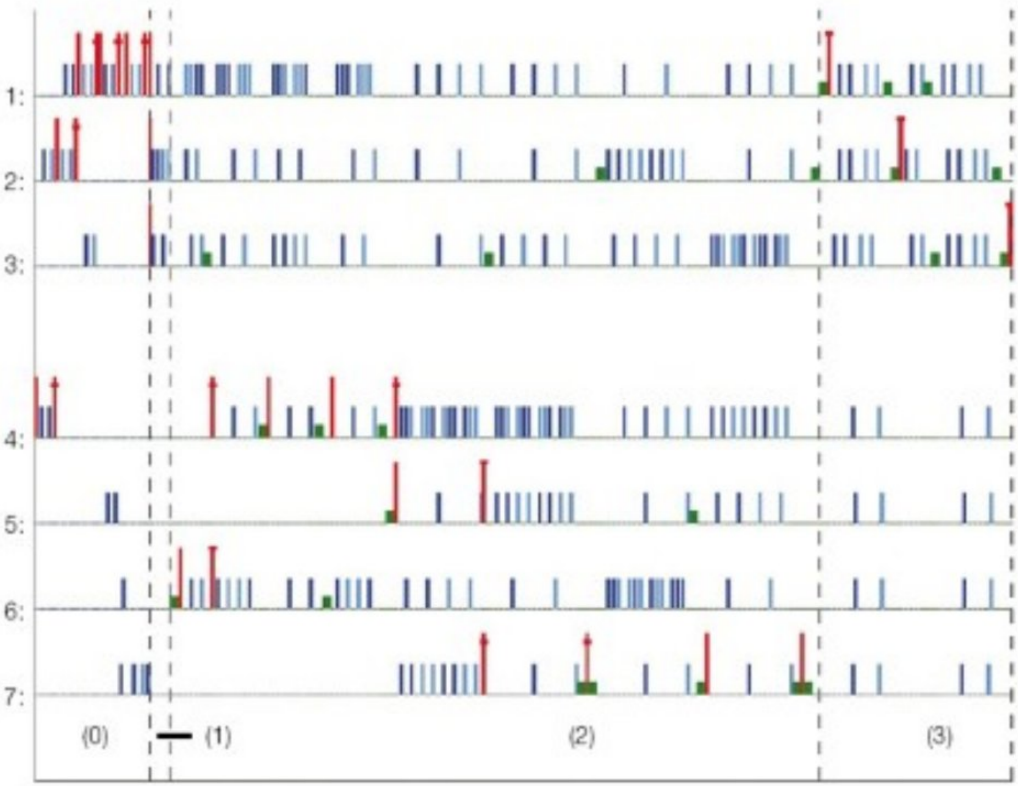
- Using $log_2 N$ more qubits, enact $f(\psi)$ on them while retaining the state ψ in the input state (output qubits)
- Apply the quantum fourier transform on the ψ portion of the circuit
- Measure the input and output qubits $(y,f(x_0))$, with high probability you will measure an of $f(x_0 + (y/N)r)$ where y/N is close to an integer

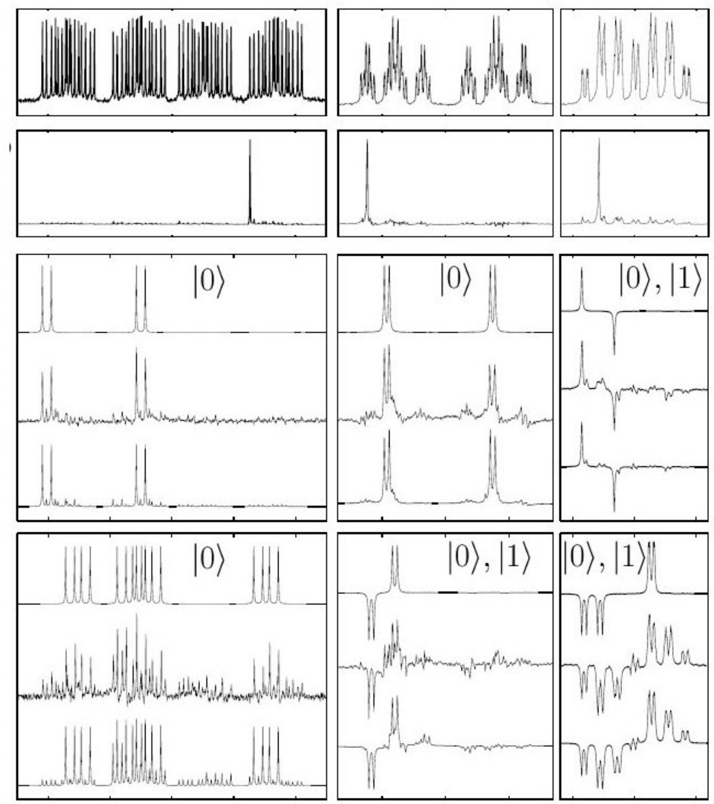


|0⟩
|0⟩
|0⟩
|0⟩
H
H
H
H
U_f
U_{QFT}^{-1}
|0⟩
|0⟩
|0⟩
|0⟩


F 1
2 F
F 3
6
7
C
C
C
C
F 4
F 5
Fe
CO
CO
C_5H_5


a
(0)
(1)
(2)
(3)
(4)
n
m
|0⟩
|1⟩
$H^{\otimes n}$
x
x
1
a^x mod N
Inverse QFT
b
1:
2:
3:
4:
5:
6:
7:
Temporal averaging
H
H
H
H
90
H
45
90
H
A
B
C
D
E
F
G
H


1:
2:
3:
4:
5:
6:
7:
(0)
(1)
(2)
(3)

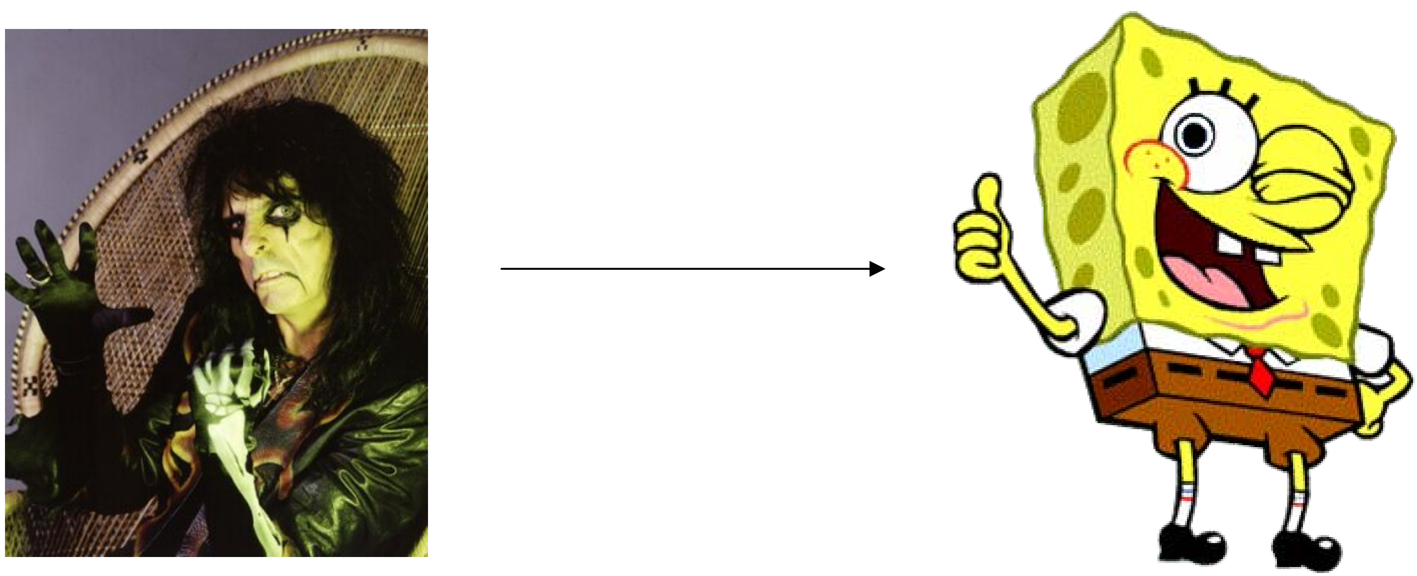

|0⟩
|0⟩
|0⟩, |1⟩
|0⟩
|0⟩, |1⟩
|0⟩, |1⟩

So we've broken it, now what?

- In general symmetric keys are harder to crack but tough to distribute, while asymmetric keys are easy to distribute but easier to crack
- Start thinking about using quantum systems to implement cryptography
- Restrictions on polarization bases measurements ($\uparrow \rightarrow \searrow \swarrow$ σ^{+} σ^{-})
- Restrictions on state duplication
- Very easy to create state perturbation

BB84 (Bennett and Brassard)

- We have two parties, Alice and Bob who want to securely distribute their symmetric key over a public channel



BB84

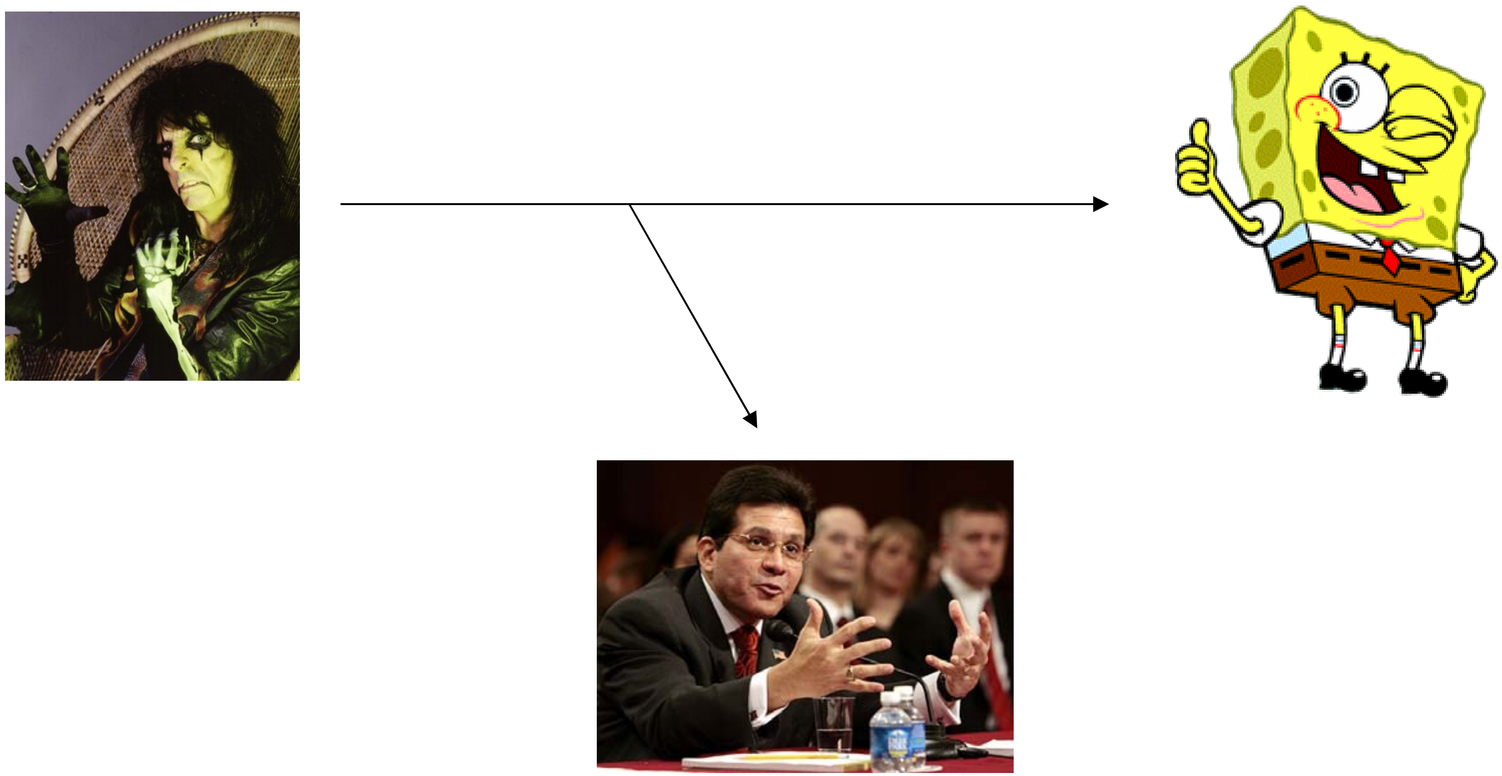
- Alice randomly chooses one of two orientations from two bases to measure in: (for spin ½ situation analogous to z-basis, and x-basis)
- Alice then assigns the value of 0 and 1 in each basis (up-z and up-x = 0, down-z and down-x =1)
- Alice sends a state from one of the four bases at random, and Bob selects (with his own random generator) a basis (x or z) to measure in
- If they choose the same basis, they will agree with 100% probability, if they choose a different basis they will have no way of correlating the results (error rate ~25%)

BB84

- In order to verify the transmitted information, Alice and Bob decide which bits can be kept and which bits will need to be retransmitted
- The correlated measurements will only be in compatible bases (both x or z)

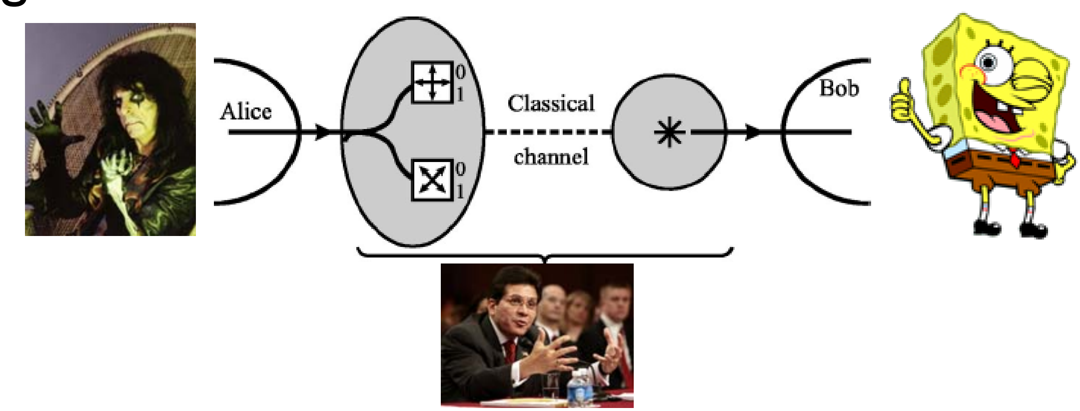
http://monet.mercersburg.edu/henle/bb84/demo.php

Eavesdropping



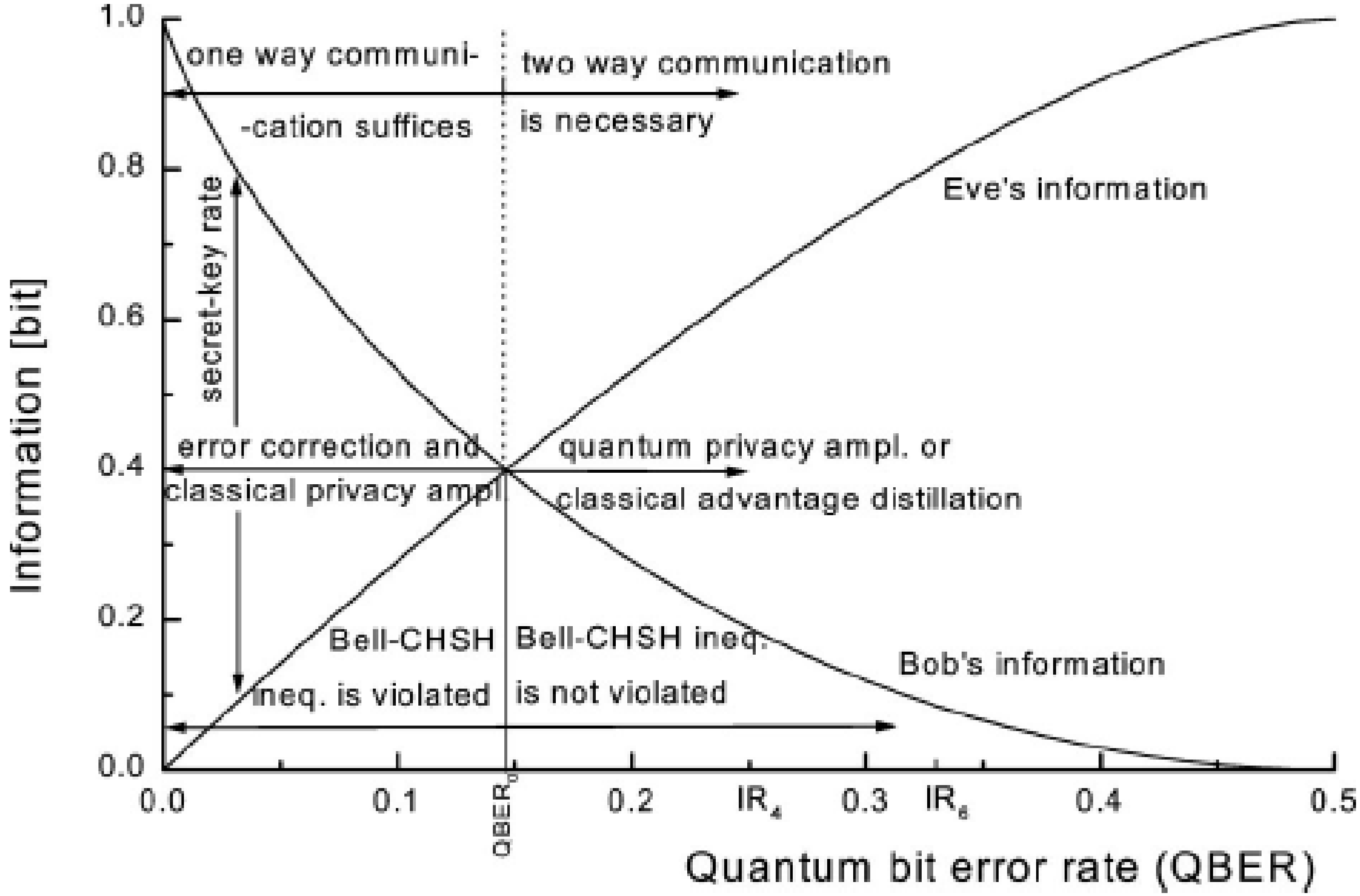
Multiple Photon Attack

- Eve can attack an optical channel by measuring multiple photon signals with a PBS and recreating the signals



2/3 of the time Eve can recreate the original state and send it to Bob, the rest of the time she introduces an error rate of 1/6

Eavesdropping Thresholds



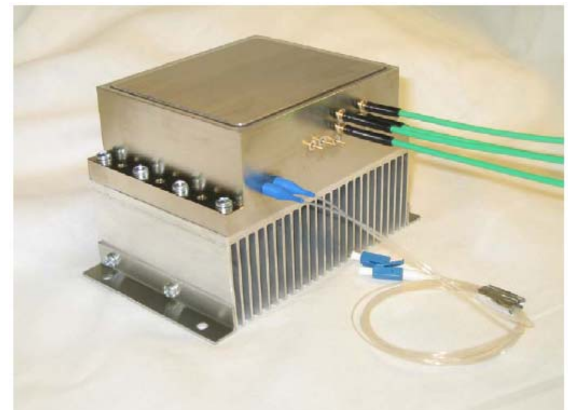
Commerical Quantum Crypto Systems

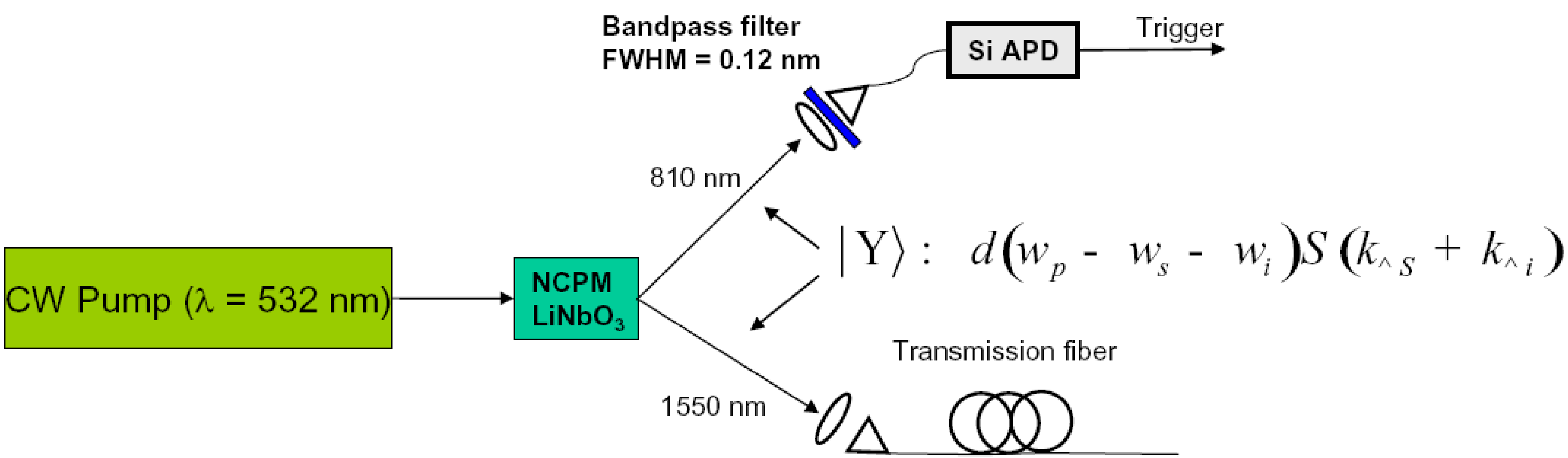
- Magiq: Currently have an implementation of a secure quantum network, the QPN 7505
- Works on a single photon source, and can transmit up to about 75 km with reasonable loss

Price? $97000

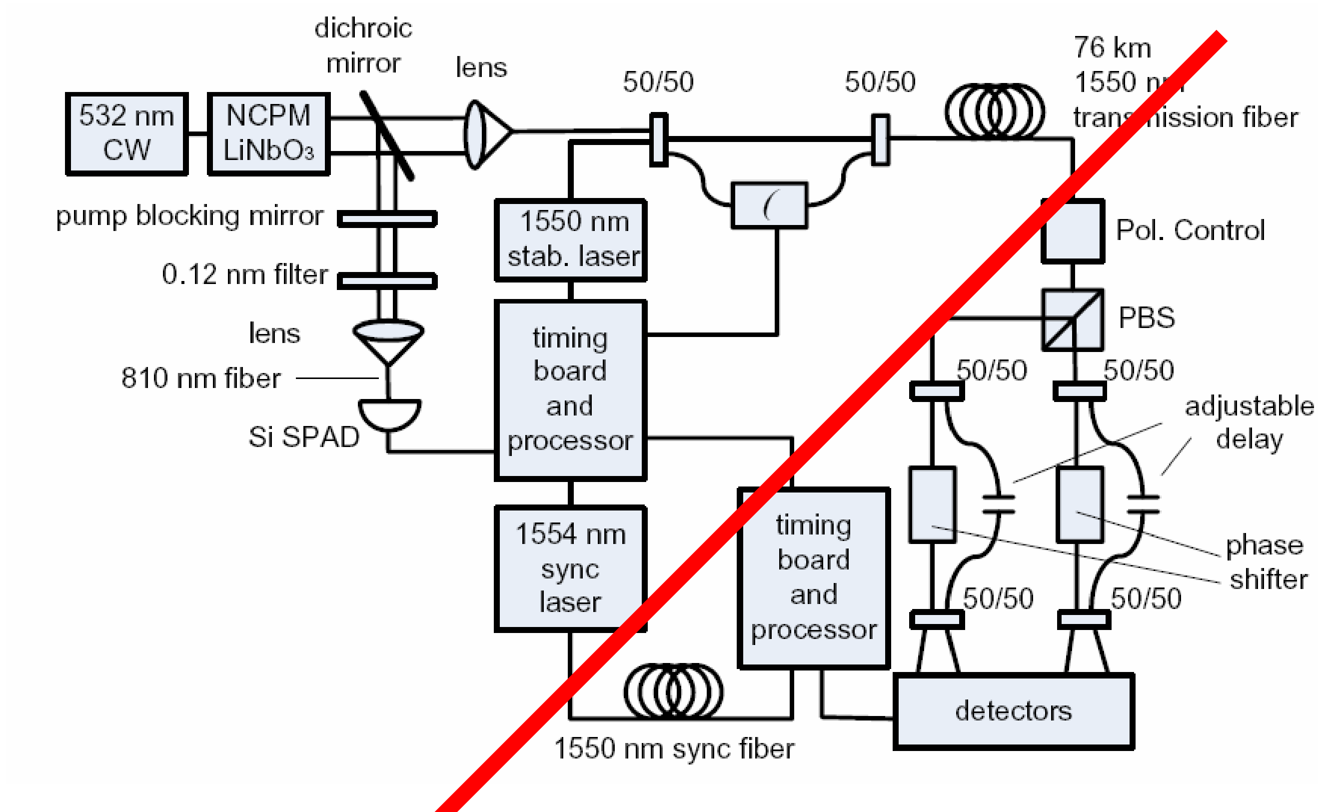
Single Photon Manipulation

Entanglement occurs in the time-frequency domain, there is a high probability that a single photon is produced, and low probability of multiple photons



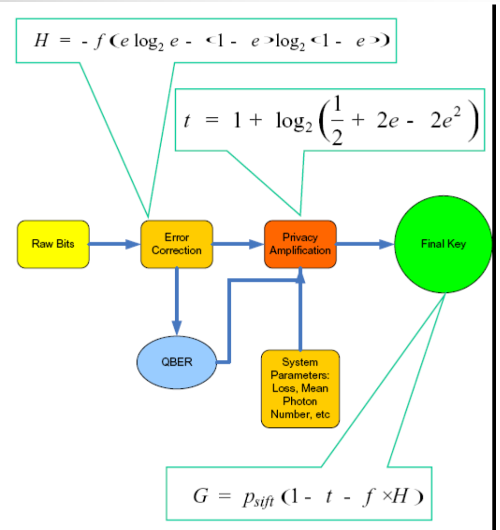


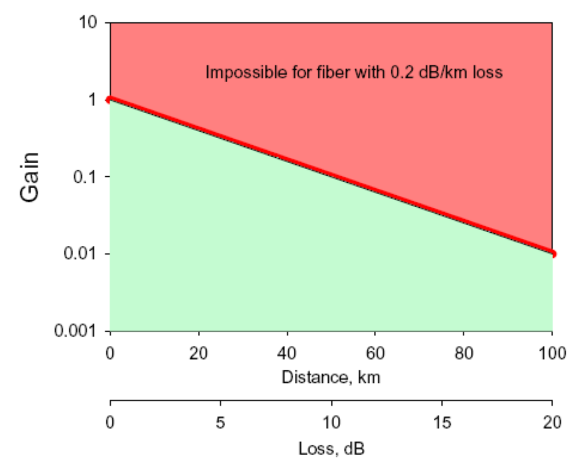
Single Photon setup



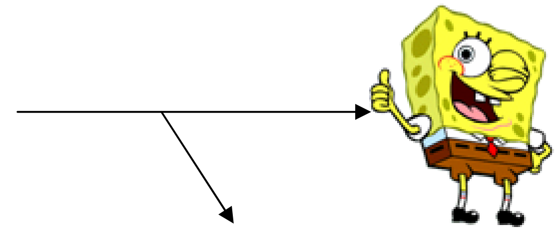
Fidelity Considerations

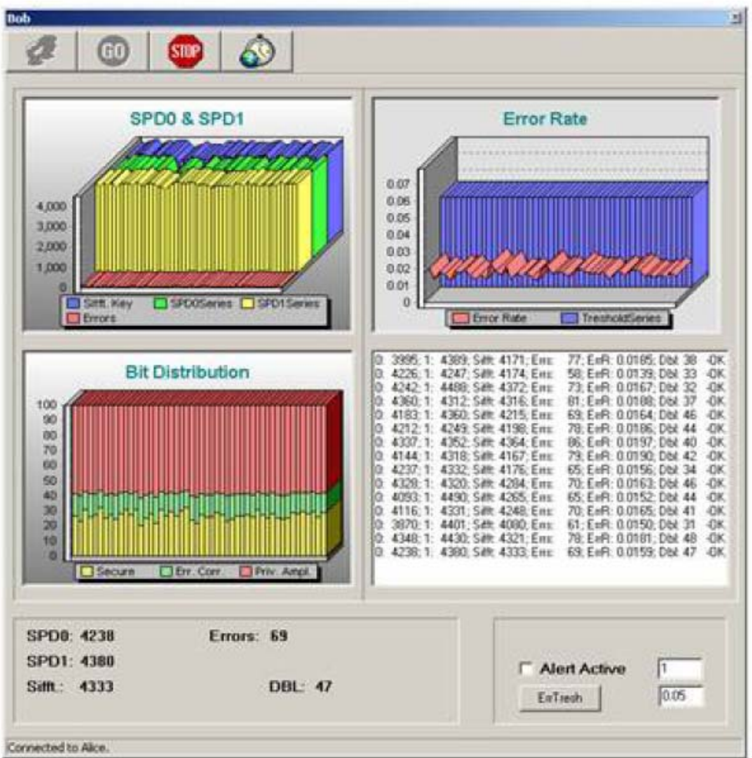
- The system tries to maximize *G*, the probability of transmitting a secure bit with a single initial pulse
- This attenuates about 10dB for every 50 km of transmission

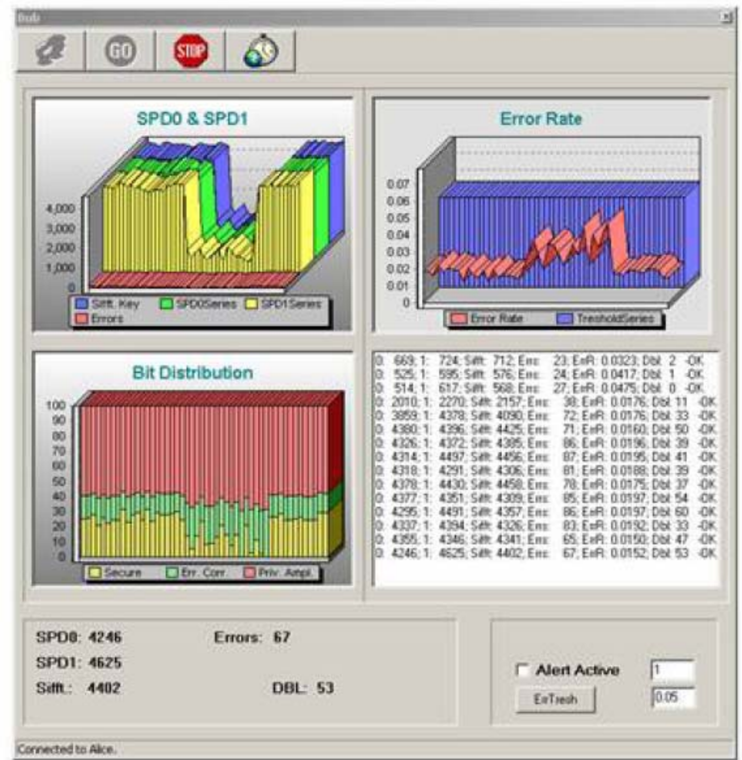




Eavesdropping!





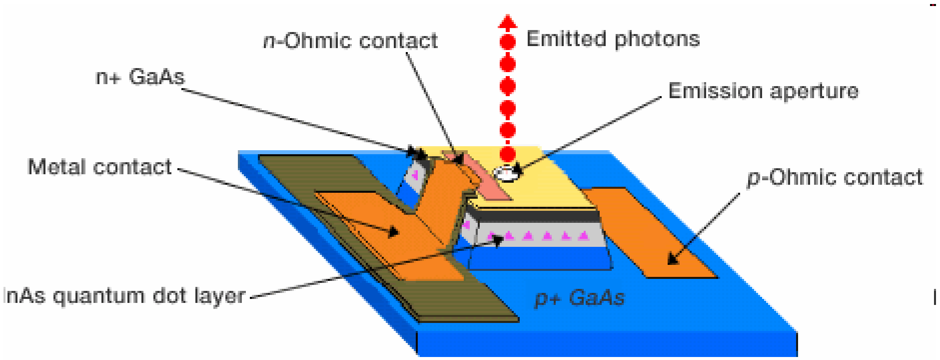


Other systems

- Id quantique:

  Vectis – Their crypto system, uses typical QKD and AES (Advanced Encryption Standard)

  Quantis – Random number generator, based on standard 50/50 polarization probabilities (4 Mbit/s number generation) PCI hardware
- Toshiba Research – Cambridge, QKD and single photon emission with quantum dots



Sources

- "*Quantum Cryptography*"; Gisin, Ribordy, Tittel, Zbinden; 2002
- "*Secure Communication with single photons*"; A. Trifonov; 2005
- "*An Overview of Cryptography*"; Gary Kessler; 2007
- "*Applications of Quantum Cryptography in Government Classified, Business, and Financial Communications*"; Audrius Berzanskis; 2005
- "*Quantum key distribution over 122 km of standard telecom fiber*"; Gobby, Yuan, Shields; 2004