

# COMPUTER & NETWORK SECURITY

Lecture 23:

**Quantum Cryptography**

**Slides originally from Vikram Sharma,  
QuintessenceLabs**



# QUANTUM CRYPTOGRAPHY

## **What is quantum cryptography?**

Using quantum computers to do cryptography

## **What are quantum computers?**

Quantum physics applied to computational tasks

## **What does quantum cryptanalysis mean for classical cryptography?**

## **Is it feasible?**

## **Can we exploit quantum effects to solve our security woes?**

## WHAT WE ARE NOT DOING

$$H(t) |\psi(t)\rangle = i\hbar \frac{d}{dt} |\psi(t)\rangle$$

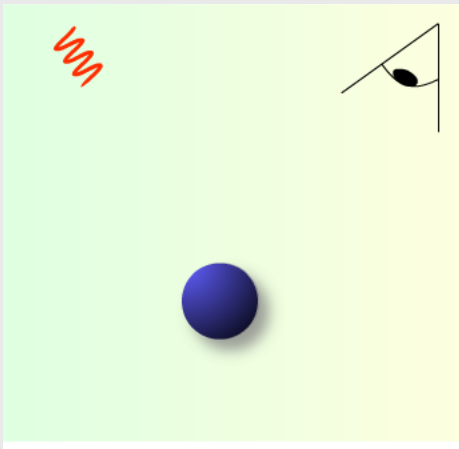
$$-\frac{\hbar^2}{2m} \frac{d^2\psi(x)}{dx^2} + U(x)\psi(x) = E\psi(x).$$

$$\mathcal{L} = \frac{i}{2} \bar{\psi} \gamma^\mu \partial_\mu \psi - \frac{i}{2} (\partial_\mu \bar{\psi}) \gamma^\mu \psi - m \bar{\psi} \psi$$

- Heisenberg Uncertainty Principle

$$\Delta x \Delta p \geq \frac{h}{4\pi}$$

- Accuracy of speed x position is limited to  $10^{-34}$  in SI Unit.
  - $\pm 0.00000000000000000000000000000001 \text{ m}^2/\text{s}$
- You cannot know everything about something



# — QUANTUM PHYSICS

- Stuff is “quantised”
  - Atoms don’t behave like little billiard balls
- Atoms emit energy in discrete quanta, called “photons”
- Atoms sometimes interact in unexpected ways
- Atomic properties are often undefined, expressed as a “superposition” of states
  - Atomic spin might be up, down, or *both*
  - Only defined when observed (“décoherence”)





## QUBITS

Classical bit

0

1

qubit

0

?

1



# HOW WE'VE BEEN DOING CRYPTO

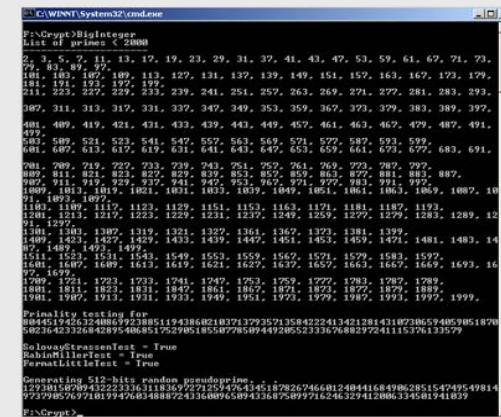
Based on complex mathematics:

- near one-way functions
- easy to compute one-way (encrypt), hard to reverse (decrypt)

$$\begin{aligned} p, q \\ n = pq \quad \phi(n) = (p-1)(q-1) \\ e, \quad 1 < e < \phi(n) \quad \gcd(e, \phi(n)) = 1 \\ d = e^{-1} \bmod \phi(n) \end{aligned}$$

Security reliant on:

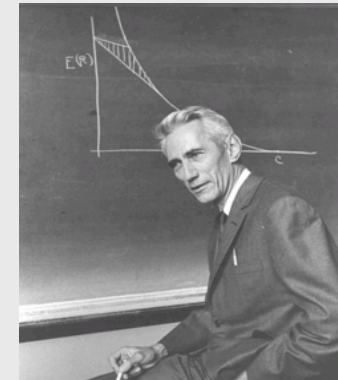
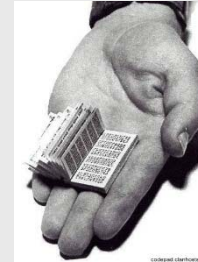
- computational intractability
- processing times of best known methods of decryption scale rapidly with the size of key
- difficulty of factoring is at the core of modern methods of encryption



```
C:\WINNT\System32\cmd.exe
P:\Crypt>BigInteger
List of primes < 2000
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73,
79, 83, 89, 97,
101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179,
181, 191, 193, 197, 199,
211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293,
307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397,
401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491,
497,
503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599,
607, 609, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691,
697,
701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797,
809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887,
897, 911, 913, 917, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997,
1009, 1013, 1019, 1021, 1031, 1033, 1039, 1047, 1051, 1061, 1063, 1069, 1087, 10
1093, 1097,
1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193,
1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1279, 1283, 1289, 12
91, 1297,
1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399,
1409, 1423, 1427, 1429, 1433, 1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 14
87, 1489, 1493, 1499,
1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597,
1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 16
97, 1699,
1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789,
1801, 1811, 1823, 1831, 1847, 1861, 1871, 1873, 1877, 1879, 1883,
1901, 1907, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999,
Primality testing for
88442194363748865923885119438682183713793571358422241342128143107386534059861870
5823642332684895486851752905185507785094492055233367688292241115376133579
SolovayStrassenTest = True
RabinMillerTest = True
FermatLittleTest = True
Generating 512-bits random pseudoprime: c
973798576971019947683488872433680965894336875899716246329412086334581941839
P:\Crypt>
```

# PERFECT SECRECY

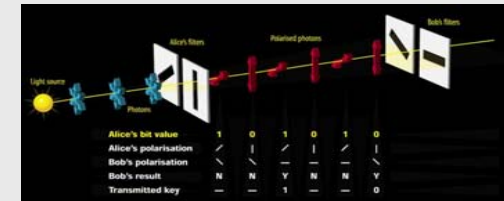
- One-Time Pad
  - based on random codes that are only used once
  - *perfect secrecy* proved by Shannon (1949)
- Problem:
  - code book (one-time pad) needs to be transported from sender to receiver
  - needs to be done securely



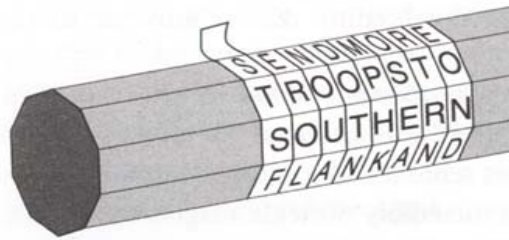


# QUANTUM CRYPTOGRAPHY

- Quantum cryptography first conceived by Brassard and Bennett (1984)
  - provides a method to transmit a one-time pad (key) using single photons
  - any eavesdropping (attempt to copy the key) results in detectable variations in quantum states of the photons
  - key can be based on true randomness drawn from nature
- Circa 2000 - proposal to use highly-tuned laser beams instead of single photons
  - ANU QOG amongst one of the first teams in the world to demonstrate a prototype
  - QuintessenceLabs developing this technology for commercial deployment



# 5<sup>TH</sup> TO 9<sup>TH</sup> CENTURY BC



5<sup>th</sup> Century BC  
Spartan scytale (wooden staff).  
Transposition cipher.

9<sup>th</sup> Century  
Earliest known description of  
frequency analysis  
Abu Yusuf Ya'qub ibn Is-haq ibn as-  
Sabbah ibn 'omran ibn Ismail al-  
Kindi  
("the philosopher of the Arabs")

Letter:	a	b	c	d	e
Percentage:	8.2	1.5	2.8	4.3	12.7

480 BC  
Greece saved from  
invasion by Persia.  
Message hidden under  
wax on wooden tablets.

Caesar cipher.  
Replace each letter with  
one 3 letters down the  
alphabet.

abcdefghijklmnopqrstuvwxyz  
DEFGHIJKLMNOPQRSTUVWXYZABC

Plaintext: veni, vidi, vici  
Ciphertext: YHQL, YLGL, YLFL

4<sup>th</sup> Century AD  
Kama-sutra art number 45  
Mlecchita-vikalpa  
Substitution cipher

A	D	H	I	K	M	O	R	S	U	W	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
V	X	B	G	J	C	Q	L	N	E	F	P	T

Meet at midnight

↕  
CUUZ VZ CGXSGIBZ

# 1200 TO 1500 AD

13<sup>th</sup> Century  
First known European book on cryptography.  
*Epistle on the Secret Works of Art and the Nullity of Magic.*  
Francis Bacon

15<sup>th</sup> Century  
European cryptography a burgeoning industry.  
Cryptanalysis beginning to emerge in Europe.

Plain	abcdefghijklmnopqrstuvwxyz
1	BCDEFGHIJKLMNOPQRSTUVWXYZA
2	CDEFGHIJKLMNOPQRSTUVWXYZAB
3	DEFGHIJKLMNOPQRSTUVWXYZABC
4	EFGHIJKLMNOPQRSTUVWXYZABCD
...	...
26	ABCDEFGHIJKLMNOPQRSTUVWXYZ

1586  
*A Treatise on Secret Writing*  
Vigenere cipher  
Polyalphabetic cipher

14<sup>th</sup> Century  
Cryptography widespread  
Geoffrey Chaucer's  
*Treatise on the Astrolabe*  
included several encrypted paragraphs.  
Substitution using symbols.

1467  
Leon Battista Alberti  
Cipher machine  
Substitution cipher



8<sup>th</sup> February, 1587  
Mary, Queen of Scots  
beheaded

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z
o	†	∧	‡	α	□	θ	∞	!	δ	κ		∅	∇	§	∩	Δ	ε	⊂	7	8	9	

Nulles ff. r. . . d. Dowbleth σ

and for with that if but where as of the from by  
 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1090 1091 1092 1093 1094 1095 1096 1097 1098 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1190 1191 1192 1193 1194 1195 1196 1197 1198 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290 1291 1292 1293 1294 1295 1296 1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1390 1391 1392 1393 1394 1395 1396 1397 1398 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1490 1491 1492 1493 1494 1495 1496 1497 1498 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1590 1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1690 1691 1692 1693 1694 1695 1696 1697 1698 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1790 1791 1792 1793 1794 1795 1796 1797 1798 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1890 1891 1892 1893 1894 1895 1896 1897 1898 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2190 2191 2192 2193 2194 2195 2196 2197 2198 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2360 2361 2362 2363 2364 2365 2366 2367 2368 2369 2370 2371 2372 2373 2374 2375 2376 2377 2378 2379 2380 2381 2382 2383 2384 2385 2386 2387 2388 2389 2390 2391 2392 2393 2394 2395 2396 2397 2398 2399 2400 2401 2402 2403 2404 2405 2406 2407 2408 2409 2410 2411 2412 2413 2414 2415 2416 2417 2418 2419 2420 2421 2422 2423 2424 2425 2426 2427 2428 2429 2430 2431 2432 2433 2434 2435 2436 2437 2438 2439 2440 2441 2442 2443 2444 2445 2446 2447 2448 2449 2450 2451 2452 2453 2454 2455 2456 2457 2458 2459 2460 2461 2462 2463 2464 2465 2466 2467 2468 2469 2470 2471 2472 2473 2474 2475 2476 2477 2478 2479 248

# 1600 TO 1800 AD

17<sup>th</sup> Century  
Homophonic cipher

a	b	c	d	e	f	...
09	48	13	01	14	10	...
12	81	41	03	16	31	...
33		62	45	24		...
47			79	44		...
53				46		...
...				...		...

18<sup>th</sup> Century  
Cryptanalysis becomes industrialised. Geheime Kabinets-Kanzlei in Vienna opened all mail passing through Austria. All monoalphabetic ciphertext messages decrypted.

Cryptographers switch to Vigenere and other polyalphabetic ciphers.

Louis XIII, Louis XIV  
The Great Cipher  
Not broken until late 19<sup>th</sup> Century  
Multi-syllabic cipher

~1854  
Charles Babbage breaks Vigenere cipher (but not published).

1863  
Friedrick Wilhelm Kasiski breaks Vigenere cipher.  
*Secret Writing and the Art of Deciphering*



# 1900 TO 1960 AD

5<sup>th</sup> March, 1918  
German ADFGVX  
cipher introduced.  
Substitution and  
transposition.

2<sup>nd</sup> June, 1918  
ADFGVX cipher  
broken by  
Georges Painvin.

1926  
German Enigma machine  
Plugboard and scramblers  
combine to provide over  
10,000,000,000,000,000 keys.

Increased to  
159,000,000,000,000,000,000 keys  
in December 1938.



1918  
Major Joseph Mauborgne  
Concept of a random key leads  
to the *One Time Pad*, perfect  
security.  
No patterns, no structure. Can  
be mathematically proven to be  
absolutely secure.

Problem: impractical to  
implement in most situations.

Post World War 2  
Programmable electronic  
machines (computers) replace  
mechanical machines.  
Becomes possible to build  
virtual encryption machines that  
are extremely complex.  
But all still rely on transposition  
and substitution to create  
ciphertext.



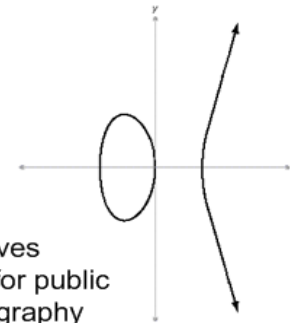
# 1970 TO 2000 AD

1970s  
Lucifer cipher  
developed at  
IBM

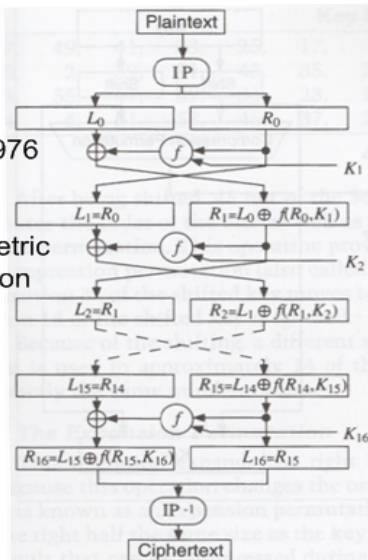
P & Q PRIME  
 $N = PQ$   
 $ED = 1 \text{ MOD } (P - 1)(Q - 1)$   
 $C = M^E \text{ MOD } N$   
 $M = C^D \text{ MOD } N$

April, 1977  
 RSA algorithm  
 Encryption and digital  
 signatures

1985  
 Elliptic curves  
 proposed for public  
 key cryptography



23 November, 1976  
 Data Encryption  
 Standard (DES)  
 56-bit key symmetric  
 algorithm based on  
 Lucifer



1976  
 Diffie-Hellman Key  
 Exchange Protocol.  
 Public key cryptography

1. Alice chooses random  $x$  and sends Bob:  
 $X = g^x \text{ mod } n$
  2. Bob chooses random  $y$  and sends Alice:  
 $Y = g^y \text{ mod } n$
  3. Alice computes:  
 $k = Y^x \text{ mod } n$
  4. Bob computes:  
 $k' = X^y \text{ mod } n$
- $k = k' = g^{xy} \text{ mod } n$

26<sup>th</sup> November, 2001  
 Advanced Encryption  
 Standard (AES)  
 128, 192, 256-bit key  
 symmetric algorithm

# ■ CLASSICAL ALGORITHMS

- Based on
  - Complex transposition and substitution
  - Hard mathematical algorithms
- Rely on
  - No algorithmic weaknesses
  - Infeasibility of brute force attack
  - Mathematical complexity
- OTP offers provably secure encryption
  - Perfect security

# ALICE, BOB & EVE

Eve is omnipresent

She is always around

Eve is omniscient

She knows all the tricks, including those we do not know

She knows our cryptography algorithm

Eve is omnipotent

She has perfect interception setups

She has infinite amount of money

She has infinite time



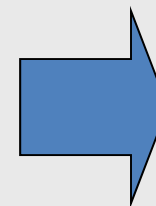
"Alice"



"Eve"



"Bob"



**Eventually  
RSA is  
insecure!!!**

# ■ 1<sup>ST</sup> INGREDIENT: RANDOMNESS

What is true randomness, what tests are there?

Why is it difficult to get random number from computers

Because it always relies on fixed algorithm

In Physics, it is dead easy:

Radioactive decay

Quantum Decoherence

Reflection of a photon off a half silvered mirror.

## ■ 2<sup>ND</sup> INGREDIENT: IRREVERSIBILITY

There is no known irreversible 1-to-1 mathematical function!  
Many-to-one functions and one-to-many relations cannot work.

Best approximation to irreversible function is factorization.  
It is easier to multiply large numbers, harder to factorize.  
It is easier to differentiate complex functions, harder to integrate.

In Physics, we can rely on concept such as **Indistinguishability**.  
In Physics, we can use **Wavefunction Collapse**

**Reduction of a superposition of eigenstates to a single eigenstate after interaction with an observer**



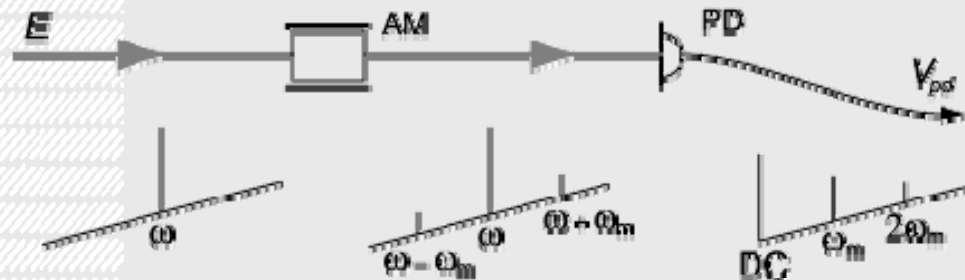
# ■ BASIC QUANTUM PHYSICS

1. Heisenberg Uncertainty Principle
2. No cloning theorem
3. Universally pervasive noise - Quantum/Vacuum noise
4. Einstein-Podolsky-Rosen entanglement and Wavefunction Collapse
5. Quieter than vacuum??

# ■ QUANTUM LASER BEAM

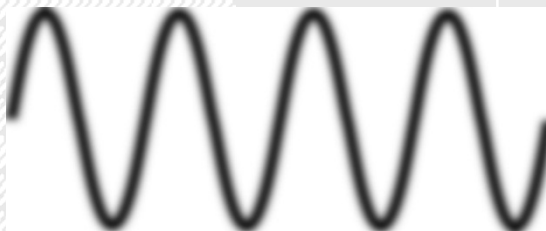
Lasers are ideal for telecommunication.

Information can be encoded by varying the amplitude and the phase of a laser: AM and FM encoding.

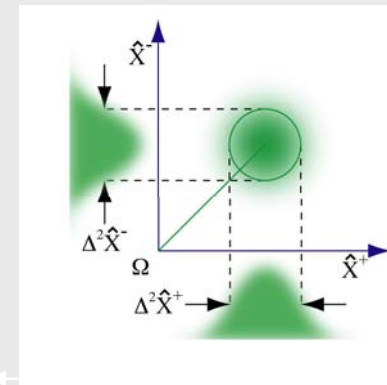


For a laser the amplitude and the phase of a laser beam cannot be simultaneously determined.

•Amplitude

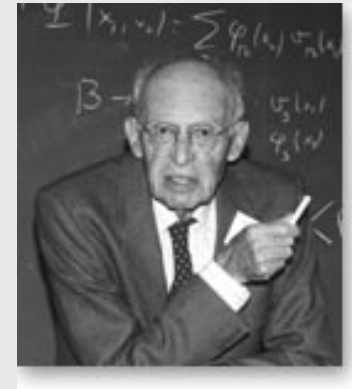
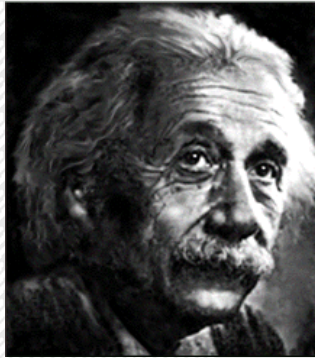


•Phase



Quantum noise can be represented by a Ball and stick diagram

# EPR ENTANGLEMENT AND WAVEFUNCTION COLLAPSE



- Entanglement means that the left hand knows what the right hand is doing, even when the hands are very far apart
- Wavefunction collapse is our 2nd ingredient
  - “a one time lock/key”.

## QKD THEORY



- Secure information

$$\Delta I = I_{AB} - I_E$$

where  $I_{AB}$  is the amount of shared information Alice and Bob can agree on and  $I_E$  is the maximum amount of information accessible to a third party with total control over the transmission channel

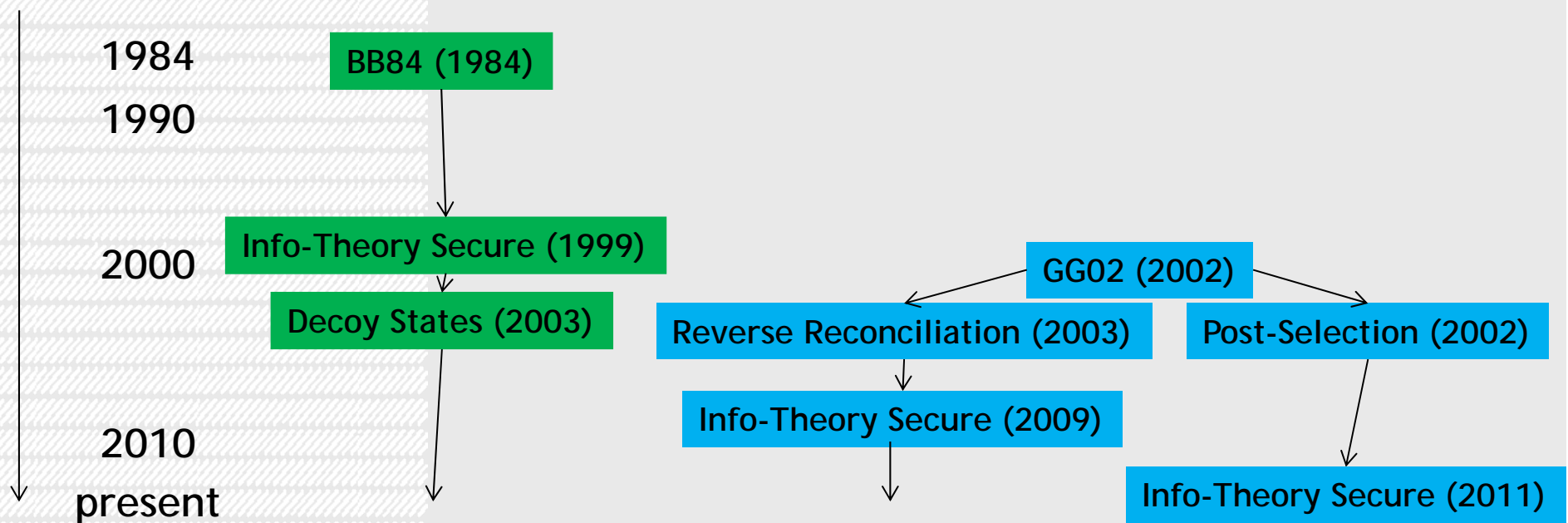
- A QKD device must:

- Estimate the channel parameters to bound  $I_E$
- Reconcile efficiently the information shared between Alice and Bob
- Extract the secure information

# TWO TYPES OF QKD

## DV-QKD

## CV-QKD



## DV-QKD

## CV-QKD

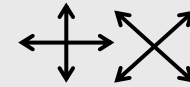
<b>Sources</b>	Single photons/ Attenuated coherent lasers	Weakly modulated bright coherent laser
<b>Detectors</b>	Single-photon detectors	Homodyne detectors



## ■ BB84: BENNETT & BRASSARD (1984)

Quantum key exchange with polarised photons

Two basis pairs of two states (rectilinear and diagonal)



Alice generates random bit string, and random basis sequence

e.g. 0110101 and

Alice sends a photon per bit, polarised with the chosen basis

Bob randomly picks a basis for each bit

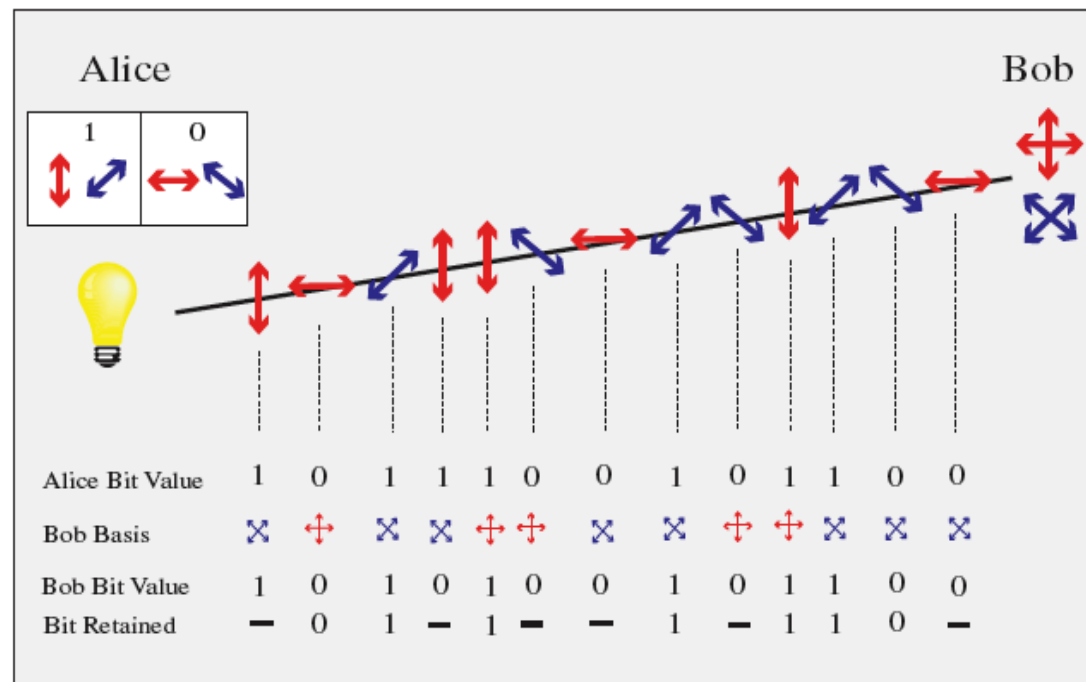
Alice and Bob compare notes later, only about chosen basis

Any interception by Eve destroys initial photon state

Immune to MITM if Alice and Bob can verify each other's identity

## ■ BB84: BENNETT & BRASSARD (1984)

Bennett and Brassard proposed in 1984 that if single photons are sent from Alice to Bob, communication between them can be absolutely secure.

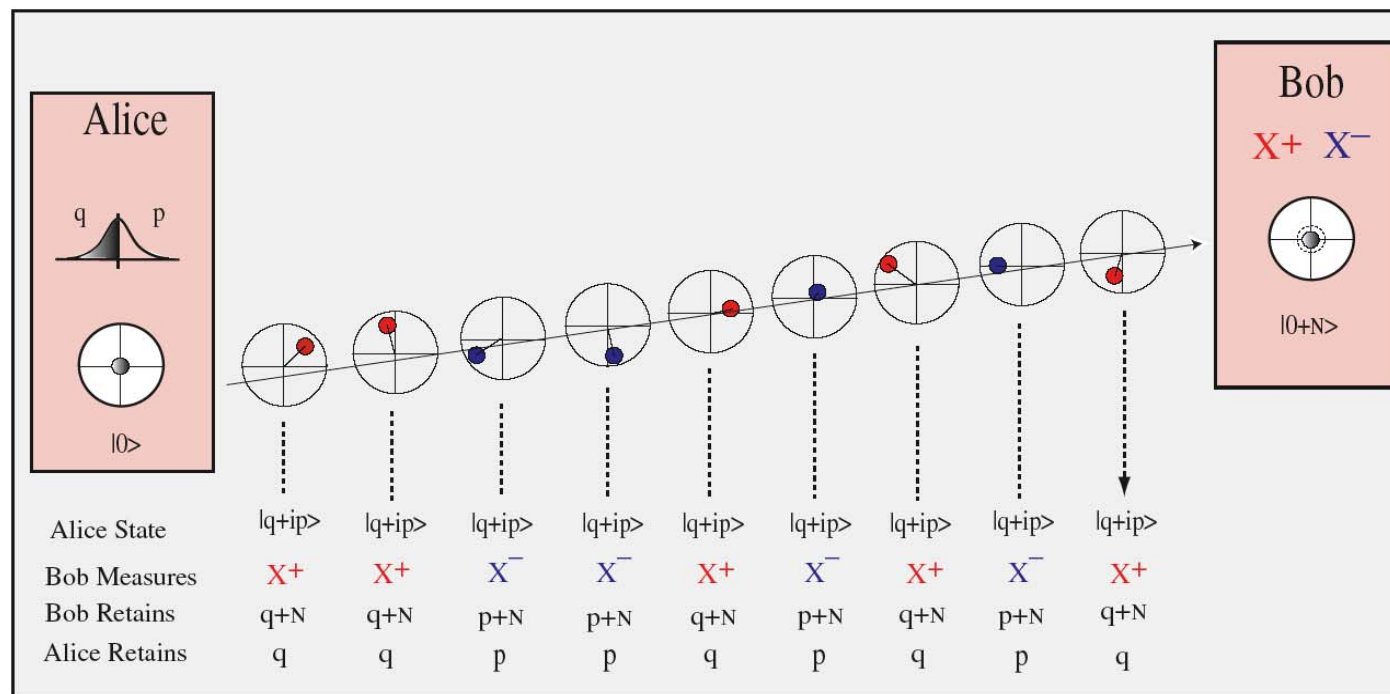


## ■ PRACTICALITY OF BB84

- **Implementations are getting better**
  - 1989: 32 cm
  - Now ~200km
  - 144km Free Space
- **Still very slow and difficult, and doesn't solve everything**
  - authentication
  - non-repudiation (digital signatures)
  - and more ...
- **Moral: there are no "silver bullets" for security problems**

# BRIGHT LASER BEAM CRYPTOGRAPHY

- Several proposals surfaced after 2000 suggested that whole laser beams can be used for quantum cryptographic communication 1989



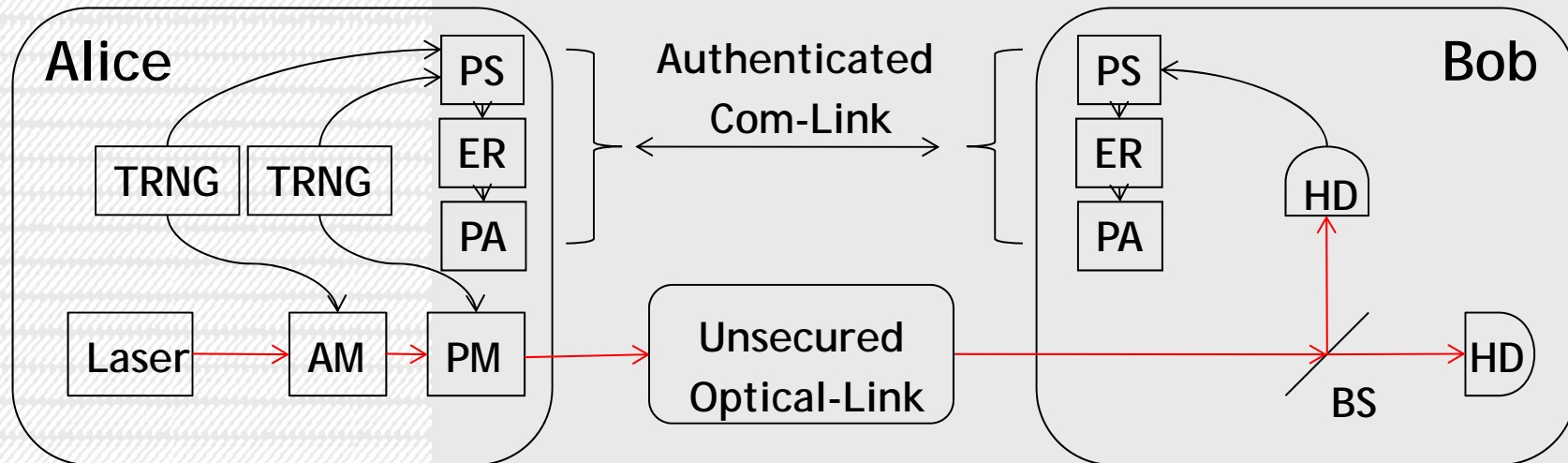
## ■ CV-QKD: ADVANTAGES

- Higher detectors efficiencies
- Off-the-shelf components
- Telecommunications compatible
- Higher key rates achievable:

	Optical Device	Bandwidth
Laser	Shot-noise-limited laser	Essentially unlimited*
Modulators	Amplitude and phase modulators	Available: >40 GHz
Detectors	Shot-noise-limited homodyne detectors	Available: 10 GHz



# CV-QKD: IMPLEMENTATION



## Optics Layout

Coherent Laser

True Random Number Generator (TRNG)

Amplitude (AM) and Phase (PM) Modulators

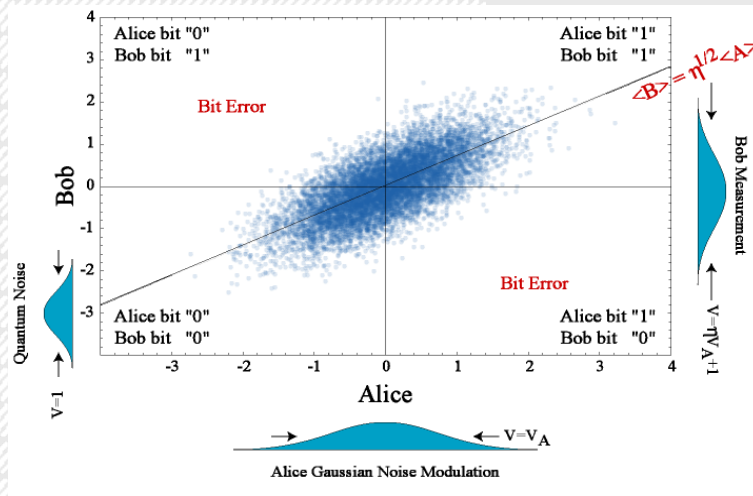
Beam-splitter (BS)

Homodyne Detectors (HD)

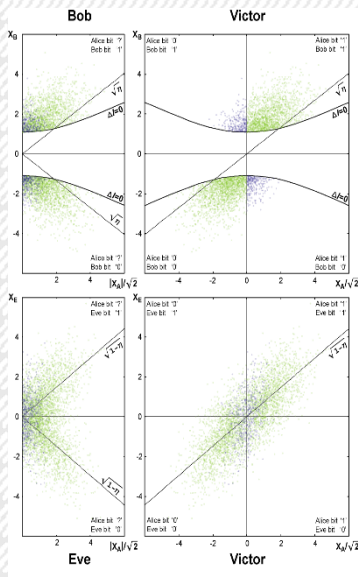
## • Post-processing

- Post-Selection (PS)
- Error Reconciliation (ER)
- Privacy Amplification (PA)

# MATHEMATICAL TRICKS



Vacuum noise  
Wave function collapse  
Post-selection  
Cascade reconciliation  
Privacy amplification



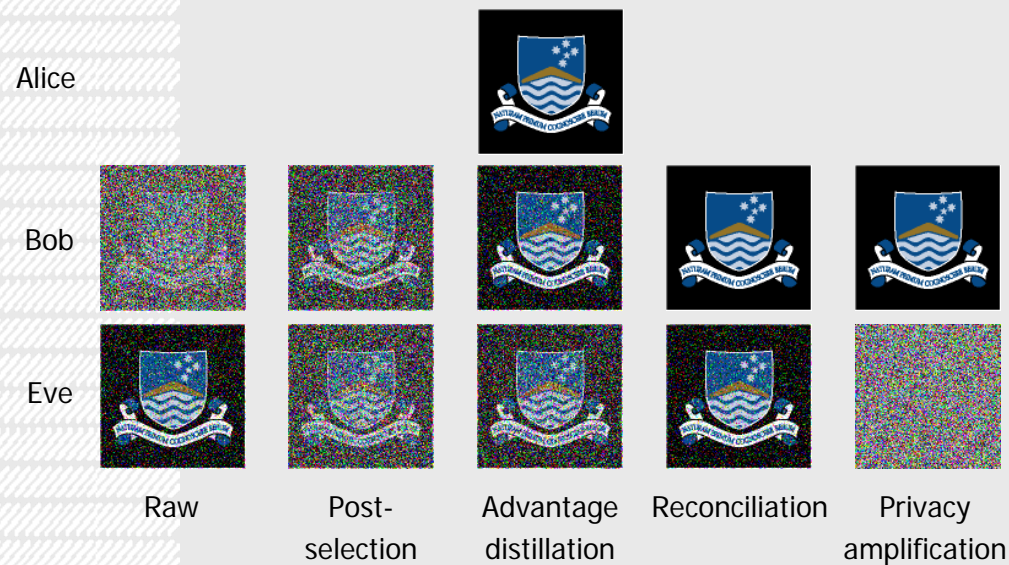
$$\left[ (1/0)x^{110503} + (1/0)x^{110502} + K + (1/0)x + (1/0) \right] \times [r_{11503}x^{110503} + K + r_0] \mod [x^{110503} + x^{5011} + 1]$$

$$[f_{110503}x^{110503} + f_{110502}x^{110502} + K + f_1x + f_0]$$



# QUANTUM NOISE ON LASER BEAMS

"It can be squarely asserted that quantum physics can offer a way to generate a cipher key which is absolutely unbreakable"



# QUBIT REGISTERS

Classical bit registers

000 100

001 101

010 110

011 111

qubits registers  
(entangled qubits)

???

# QUBIT COMPUTATION

$F(X) = 2 * X \text{ (MOD 8)}$

Classical bits

000	001	101
↓	↓	↓
000	010	010

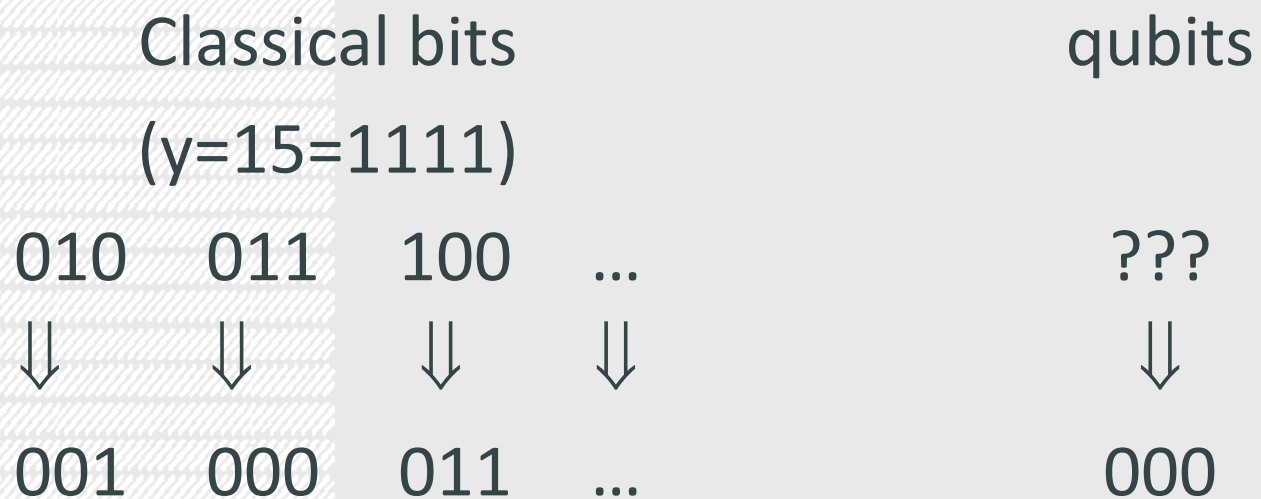
qubits

???
↓
??0



# QUBIT COMPUTATION (FACTORING Y)

$F(X) = Y \text{ MOD } X$



# SHOR'S ALGORITHM

Peter Shor, AT&T (1994)

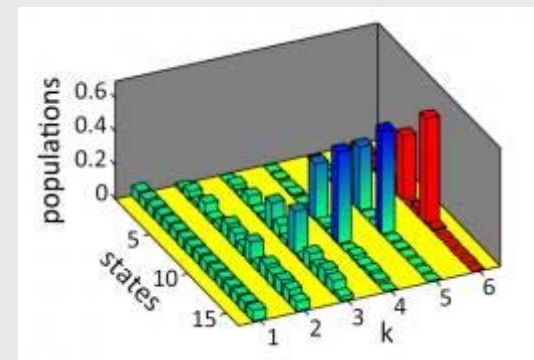
Factors in  $O((\log N)^3)$

Efficient factoring of  $n$ -bit integers with  $2n$ -qubit registers

The efficiency of Shor's algorithm is due to the efficiency of the quantum Fourier transform, and modular exponentiation by repeated squarings.

Chinese researchers implemented the largest so far

Factored 143 into  $11 * 13$



# ■ QUANTUM COMPUTER COMPLEXITY

BQP (Bounded-error, Quantum, Polynomial time)

“the class of decision problems solvable by a quantum computer in polynomial time, with an error probability of at most 1/3 for all instances” – equivalent of BPP

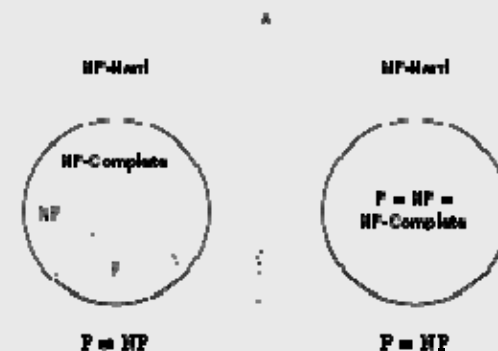
$P \subseteq BQP$

NP-complete ? BQP (probably disjoint)

Primality testing  $\in P$  [Agrawal et al, 2004]

Integer factorisation  $\in BQP$  [Shor, 1994]

P vs NP: Informally, it asks whether every problem whose solution can be quickly verified by a computer can also be quickly solved by a computer



## ■ IMPLICATIONS

- Anything relying on integer factorisation or the discrete logarithm problem can't resist quantum cryptanalysis  
RSA, DSA, Diffie-Hellman, El Gamal, ECC
- One-Time Pad is still fine – why?
- Quantum cryptography offers the possibility of perfect secrecy that cannot be compromised by advances in computational or mathematical capabilities

# ■ REFERENCES

Quantiki

[www.quantiki.org](http://www.quantiki.org)