Using Qubits to Qu$_{\text{rack}}$ the Uncrackable

VNU CVN GNL OCH

CT WH CT PC SO KH

_depar_tment_ofphy_sicsa_ndast_ronom_
_yuniv_ersit_yofke_ntuck_ylexi_ngton_

Cryptology

	SKBVL FVLVE LJIXQ	Cipher Text
Caesar shift ± 3:	$\Downarrow$ $\Downarrow$ $\Downarrow$	**DECRYPT**
	physi_cs|is|b_ig|fun	Plain Text
Substitution:	$\Downarrow$ $\Downarrow$ $\Downarrow$	**ENCRYPT**
	YGFWC PWCWT CRSXH	Cipher Text′

Encryption/Decryption: $\boxed{\pm 3}$ **Key**

$$\{\ldots, \mathtt{h} \Leftrightarrow \mathtt{G}, \ldots, \mathtt{p} \Leftrightarrow \mathtt{Y}, \ldots\}$$

---

a b c d e f g h i j k l m n o p q r s t u v w x y z

$\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ **ENCRYPTION** $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$

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

$\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ **DECRYPTION** $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$

a b c d e f g h i j k l m n o p q r s t u v w x y z

TJPNX WJNBZ OCPTJ GNUCZ LCWWZ XHDCE JZLVC HNLFJ
MYJLC JHPJC BCWUJ LFVCS SCPXD BBZRJ BXWJV BZNHV
CBNYY JNLWY JPXDC NLNHV OFWBJ LCZXW BZJUJ LFZHJ
TZBGB ZBGJH ZUCPJ NHVBZ BGJJM YJLCJ HPJVY GFWCP
CWBJU JHBGJ JMYJL BWVZH ZBXHV JLWBN HVCBB GJINF
BGJFI ZXDVD CEJBZ NHVCB CWYJL SJPBD FLJNW ZHNTD
JBGNB BGJFW GZXDV HZBTJ PNXWJ NDDZS VCLJP BGXON
HJMYJ LCJHP JNHVZ SGXON HCHBX CBCZH NYYDC JWBZD
NLRJZ TAJPB WIJEH ZIGZI DNLRJ ZTAJP BWICD DNPBT
XBBGC HRWZH NWOND DWPND JAXWB VZHZB NPBBG NBINF
WZIJG NUJBZ DJNLH NTZXB BGJOC HNWZL BZSNT WBLNP
BZLCO NRCHN BCUJS NWGCZ HNHVH ZBTFP ZHHJP BCZHI
CBGZX LVCLJ PBJMY JLCJH PJLYS

$\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$

Frequency count:

e	t	a $\longleftrightarrow$	o	i	n	s ...
J–**63**	B–**54**	Z–**42**	N–**41**	C–**38**	H–**36**	W–**27**
L–**25**	P–**22**	G–**20**	D–**19**	V–**18**	X–**17**	Y–**12**
T–**11**	F–**11**	I– **9**	U– **7**	S– **7**	O– **7**	R– **5**
M– **5**	Q– **3**	E– **3**	A– **3**	K– **0**		

$\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$

TePaX seato OiPTe GaUio Lisso XnDiE eoLVi naLFe
MYeLi enPei tisUe LFViS SiPXD ttoRe tXseV toanV
itaYY eaLsY ePXDi aLanV OFste LioXs toeUe LFone
TotGt otGen oUiPe anVto tGeeM YeLie nPeVY GFsiP
isteU entGe eMYeL tsVon otXnV eLsta nVitt GeIaF
tGeFI oXDVD iEeto anVit isYeL SePtD FLeas onaTD
etGat tGeFs GoXDV notTe PaXse aDDoS ViLeP tGXOa
neMYe LienP eanVo SGXOa nintX ition aYYDi estoD
aLReo TAePt sIeEn oIGoI DaLRe oTAeP tsIiD DaPtT
XttGi nRson asOaD DsPaD eAXst Vonot aPttG atIaF
soIeG aUeto DeaLn aToXt tGeOi nasoL toSaT stLaP
toLiO aRina tiUeS asGio nanVn otTFP onneP tionI
itGoX LViLe PteMY eLien PeLYS

⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓

Monoalphabetic substitution:

N	T	P	V	J	S	R	G	C	A	E	D	O	H	Z	Y	K	L	W	B	X	U	I	M	F	Q
⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

becau_se ato_mic be_havio_r is so_unlik_e ordi_nary e_
xperi_ence i_t is ve_ry dif_ficul_t to ge_t used_to and_
it app_ears p_eculi_ar and_myste_rious_to eve_ryone_
both t_o the n_ovice_and to_the ex_perie_nced p_hysic_
ist ev_en the_exper_ts do n_ot und_ersta_nd it t_he way_
they w_ould l_ike to_and it_is per_fectl_y reas_onabl_
e that_they s_hould_not be_cause_all of_direc_t huma_
n expe_rienc_e and o_f huma_n intu_ition_appli_es to l_
arge o_bject_s we kn_ow how_large_objec_ts wil_l act b_
ut thi_ngs on_a smal_l scal_e just_do not_act th_at way_
so we h_ave to_learn_about_them i_n a sor_t of ab_strac_
t or im_agina_tive f_ashio_n and n_ot by c_onnec_tion w_
ith ou_r dire_ct exp_erien_ce rpf_____

Because atomic behavior is so unlike ordinary experience, it is very difficult to get used to, and it appears peculiar and mysterious to everyone–both to the novice and to the experienced physicist. Even the experts do not understand it the way they would like to, and it is perfectly reasonable that they should not, because all of direct, human experience and of human intuition applies to large objects. We know how large objects will act, but things on a small scale just do not act that way. So we have to learn about them in a sort of abstract or imaginative fashion and not by connection with our direct experience.

—Richard P. Feynman, *The Feynman Lectures*, vol. 3, p. 1–1

Public **en/decryption algorithm** *vs.* ***Private*** **symmetric key**

Steganography — just *hide* the message!

One-Time Pads — TRULY SECURE ... *if* indeed *one*time

Scramble

$\Longrightarrow$

Plain Text — **Key** — Cipher Text

$\Longleftarrow$

Unscramble

Simple Shifts, Substitutions —

- ¿ Caesar shifts ..... HFJXFW XMNKYX
- ¿ Monoalphabetic substitutions ..... WXTWBCBXBCZHW
  Ciphers ..... 

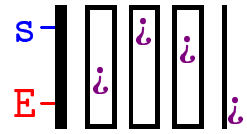
Keyed Transpositions &/or Substitutions —

- ¿ Vigenère Square (*Le Chiffre Indéchiffrable*) .....
- ¿ Playfair Cipher (SH MV CM KQ), &c.

Key	a	b	c	d	···
A= 1	A	B	C	D	···
T=20	T	U	V	W	···
O= 9	O	P	Q	R	···
M=14	M	N	O	P	···
⋮	⋮	⋮	⋮	⋮	⋱

Substitutions + Transpositions $\Longrightarrow$ Hyper-Scrambling —

- ¿ Cipher
- ¿ Enigma .....
- ¿ Lucifer **[DES]** ..... $16 \times \{B_n = B_{n-2} + \underline{\texttt{Scramble}}(B_{n-1})\}$ (4 bytes) (56-bit key)



¡¡¡ **Key** **Distribution Problem** !!!

Modular Arithmetic$_1$—A "Natural" Scrambler

Modular Arithmetic —A One-Way Function (in effect)

prime p

$\downarrow$

$$\left.\begin{array}{l}
3^0 \bmod 7 = 1 \bmod 7 = 1 \\
3^1 \bmod 7 = 3 \bmod 7 = 3 \\
3^2 \bmod 7 = 9 \bmod 7 = 2 \\
3^3 \bmod 7 = 6 \bmod 7 = 6 \\
3^4 \bmod 7 = 18 \bmod 7 = 4 \\
3^5 \bmod 7 = 12 \bmod 7 = 5 \\
3^6 \bmod 7 = 15 \bmod 7 = 1
\end{array}\right\} = 1 \textbf{ period} = p - 1 \ (= 6) \text{ factors}$$

$$\begin{array}{l}
3^7 \bmod 7 = 3 \bmod 7 = 3 \\
\vdots \\
3^{6x+1} \bmod 7 = 3 \bmod 7 = 3 \\
\vdots
\end{array}$$

$\boxed{?}$

$\{1, 2, 3, 4, 5, 6\}$ form a *group* under "multiplication mod[ulo] 7"

N.B. $7 \bmod 7 = 0$

$\mu^{p-1} \bmod p = 1$

$\mu^p \bmod p = \mu$

(*"Fermat's Little Theorem"*)

It would take $\sim \mathcal{O}(p-1) \sim \mathcal{O}(6)$ attempts to extract the **exponent** from the **remainder**.

All periods mod[ulo] 7:

$$\begin{array}{lllllllll}
1^0 = 1 & 1^1 = 1 & 1^2 = 1 & 1^3 = 1 & 1^4 = 1 & 1^5 = 1 & 1^6 = 1 & 1^7 = 1 \\
2^0 = 1 & 2^1 = 2 & 2^2 = 4 & 2^3 = 1 & 2^4 = 2 & 2^5 = 4 & 2^6 = 1 & 2^7 = 2 \\
3^0 = 1 & 3^1 = 3 & 3^2 = 2 & 3^3 = 6 & 3^4 = 4 & 3^5 = 5 & 3^6 = 1 & 3^7 = 3 \\
4^0 = 1 & 4^1 = 4 & 4^2 = 2 & 4^3 = 1 & 4^4 = 4 & 4^5 = 2 & 4^6 = 1 & 4^7 = 4 \\
5^0 = 1 & 5^1 = 5 & 5^2 = 4 & 5^3 = 6 & 5^4 = 2 & 5^5 = 3 & 5^6 = 1 & 5^7 = 5 \\
6^0 = 1 & 6^1 = 6 & 6^2 = 1 & 6^3 = 6 & 6^4 = 1 & 6^5 = 6 & 6^6 = 1 & 6^7 = 6
\end{array}$$

$p - 1 \ (= 6)$ factors $\geq$ ***1 period***

$$\boxed{\{\textit{anything}\}^{6x+1} \bmod 7 = \{\textit{anything}\}}$$

Modular Arithmetic$_2$—A "Natural" Scrambler

Modular Arithmetic —A One-Way Function (in effect)

$$
\begin{array}{lll}
 & \textit{prime } p & \\
 & \downarrow & \\
909556943^{0} & \bmod 827293847003885557 = & 1 \\
909556943^{1} & \bmod 827293847003885557 = & 909556943 \\
909556943^{2} & \bmod 827293847003885557 = & 827293832559505249 \\
909556943^{3} & \bmod 827293847003885557 = & 98715155588290468 \\
909556943^{4} & \bmod 827293847003885557 = & 162073037159014500 \\
909556943^{5} & \bmod 827293847003885557 = & 362947893031370513 \\
909556943^{6} & \bmod 827293847003885557 = & 448963170571387818 \\
909556943^{7} & \bmod 827293847003885557 = & 772887992060989965 \\
 & \vdots & \\
909556943^{1006} & \bmod 827293847003885557 = & 792676866866748139 \\
909556943^{1007} & \bmod 827293847003885557 = & 51766899375757845 \\
909556943^{1008} & \bmod 827293847003885557 = & 718652652618405908 \\
 & \vdots & \\
909556943^{p-2} & \bmod 827293847003885557 = & 369739325141372446 \\
909556943^{p-1} & \bmod 827293847003885557 = & 1 \\
 & \vdots & \\
909556943^{(p-1)x+1} & \bmod 827293847003885557 = & 909556943 \\
 & \vdots & \\
 & \boxed{?} &
\end{array}
$$

$= 1$ *period*

$= p - 1$ factors

It would take $\sim \mathcal{O}(p) \sim \mathcal{O}\big(2^{\overbrace{\log_2 p}^{N\sim 60 \text{ bits}}}\big) \sim \mathcal{O}\big(10^{18}\big)$ attempts to extract the **exponent** from the **remainder**!

$$\boxed{\{\textit{anything}\}^{(p-1)\cdot[\text{ANYTHING}]+1} \bmod p = \{\textit{anything}\}}$$

A *Public* Scheme — Public-Key Cryptography!

(Diffie, Hellman, Merkle, 1977) (Alice, Bob, Eve, 200■)

$$\boxed{(\mu^{\alpha})^{\beta} \bmod p = (\mu^{\beta})^{\alpha} \bmod p}$$

¿ Alice & Bob ***publicly*** agree on part of a **key** = a huge prime # p,

e.g., $p = 827293847003885557$

¿ ... and Alice & Bob ***publicly*** agree on another part = a huge # μ,

e.g., $\mu = 909556943$

¿ Now Alice ***privately*** chooses her sub-key $\alpha = ?$ and calculates and ***publishes*** $\boxed{A = \mu^{\alpha} \bmod p}$ ... e.g.,

$$909556943^{\alpha} \bmod 827293847003885557 = \underbrace{754904643945497026}_{\text{Eve cannot determine } \alpha\,!} \equiv A$$

¿ Now Bob ***privately*** chooses his sub-key $\beta = ?$ and calculates and ***publishes*** $\boxed{B = \mu^{\beta} \bmod p}$ ... e.g.,

$$909556943^{\beta} \bmod 827293847003885557 = \underbrace{719753132956248328}_{\text{Eve cannot determine } \beta\,!!} \equiv B$$

¿ Lastly, Alice determines ***the private key*** using her α via $\boxed{B^{\alpha} \bmod p}$

& Bob determines ***the same private key*** using his β via $\boxed{A^{\beta} \bmod p}$

... e.g.,

$$719753132956248328^{\alpha} \bmod p = 754904643945497026^{\beta} \bmod p$$

$$= \underbrace{\boxed{51766899375757845}}_{\text{Eve cannot deduce this!!!}} \equiv \text{private } \boxed{\text{Key}} \text{ !!!}$$

$\boxed{\text{DES}} \Longleftarrow$ $\Downarrow$ **Lucifer**

Example$_3$ of Arithmetic modulo $(prime \times prime')$

μ ⇓ exponent

$p = 7 \quad \& \quad q = 5$

period $\leq (p-1)(q-1) = 24$

μ^{exponent} mod (35)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	2	4	8	16	32	29	23	11	22	9	18	1	2	4	8	16	32	29	23	11	22	9	18	1	2
1	3	9	27	11	33	29	17	16	13	4	12	1	3	9	27	11	33	29	17	16	13	4	12	1	3
1	4	16	29	11	9	1	4	16	29	11	9	1	4	16	29	11	9	1	4	16	29	11	9	1	4
1	5	25	20	30	10	15	5	25	20	30	10	15	5	25	20	30	10	15	5	25	20	30	10	15	5
1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6
1	7	14	28	21	7	14	28	21	7	14	28	21	7	14	28	21	7	14	28	21	7	14	28	21	7
1	8	29	22	1	8	29	22	1	8	29	22	1	8	29	22	1	8	29	22	1	8	29	22	1	8
1	9	11	29	16	4	1	9	11	29	16	4	1	9	11	29	16	4	1	9	11	29	16	4	1	9
1	10	30	20	25	5	15	10	30	20	25	5	15	10	30	20	25	5	15	10	30	20	25	5	15	10
1	11	16	1	11	16	1	11	16	1	11	16	1	11	16	1	11	16	1	11	16	1	11	16	1	11
1	12	4	13	16	17	29	33	11	27	9	3	1	12	4	13	16	17	29	33	11	27	9	3	1	12
1	13	29	27	1	13	29	27	1	13	29	27	1	13	29	27	1	13	29	27	1	13	29	27	1	13
1	14	21	14	21	14	21	14	21	14	21	14	21	14	21	14	21	14	21	14	21	14	21	14	21	14
1	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15
1	16	11	1	16	11	1	16	11	1	16	11	1	16	11	1	16	11	1	16	11	1	16	11	1	16
1	17	9	13	11	12	29	3	16	27	4	33	1	17	9	13	11	12	29	3	16	27	4	33	1	17
1	18	9	22	11	23	29	32	16	8	4	2	1	18	9	22	11	23	29	32	16	8	4	2	1	18
1	19	11	34	16	24	1	19	11	34	16	24	1	19	11	34	16	24	1	19	11	34	16	24	1	19
1	20	15	20	15	20	15	20	15	20	15	20	15	20	15	20	15	20	15	20	15	20	15	20	15	20
1	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21
1	22	29	8	1	22	29	8	1	22	29	8	1	22	29	8	1	22	29	8	1	22	29	8	1	22
1	23	4	22	16	18	29	2	11	8	9	32	1	23	4	22	16	18	29	2	11	8	9	32	1	23
1	24	16	34	11	19	1	24	16	34	11	19	1	24	16	34	11	19	1	24	16	34	11	19	1	24
1	25	30	15	25	30	15	25	30	15	25	30	15	25	30	15	25	30	15	25	30	15	25	30	15	25
1	26	11	6	16	31	1	26	11	6	16	31	1	26	11	6	16	31	1	26	11	6	16	31	1	26
1	27	29	13	1	27	29	13	1	27	29	13	1	27	29	13	1	27	29	13	1	27	29	13	1	27
1	28	14	7	21	28	14	7	21	28	14	7	21	28	14	7	21	28	14	7	21	28	14	7	21	28
1	29	1	29	1	29	1	29	1	29	1	29	1	29	1	29	1	29	1	29	1	29	1	29	1	29
1	30	25	15	30	25	15	30	25	15	30	25	15	30	25	15	30	25	15	30	25	15	30	25	15	30
1	31	16	6	11	26	1	31	16	6	11	26	1	31	16	6	11	26	1	31	16	6	11	26	1	31
1	32	9	8	11	2	29	18	16	22	4	23	1	32	9	8	11	2	29	18	16	22	4	23	1	32
1	33	4	27	16	3	29	12	11	13	9	17	1	33	4	27	16	3	29	12	11	13	9	17	1	33
1	34	1	34	1	34	1	34	1	34	1	34	1	34	1	34	1	34	1	34	1	34	1	34	1	34

Relatively prime to $pq = 35$ **Not Relatively prime to $pq = 35$**

The "Perfect" Scheme: An *Asymmetric* Public/Private Key

(Ellis $<$ 1970, Cocks & Williamson $\leq$ 1974; Diffie 1975)
(Rivest, Shamir, Adelman, 1977)

Consider again ...

$$\boxed{\{\boldsymbol{anything}\}^{(p-1)\cdot[\text{ANYTHING}]+1} \bmod p = \{\boldsymbol{anything}\}}$$

1) Alice picks ***TWO*** huge primes, p & q, and defines $\boxed{K = p \times q}$

2) Alice notes that

$$\boxed{\{\boldsymbol{anything}\}^{(p-1)(q-1)\cdot[\text{ANYTHING}]+1} \bmod (pq) = \{\boldsymbol{anything}\}}$$

She picks any huge α & β that satisfy

$$\boxed{\alpha\cdot\beta = (p-1)(q-1)\cdot[\text{ANYTHING}] + 1}\ \star$$

which is always possible if $\gcd\big((p-1)(q-1),\ \beta\big) = 1$.

3) Alice ***publishes*** her **Public Key** $= \boxed{\{K, \beta\}}$

without, however, revealing p & q !

$\star\star\star\star\star$ ***It's practically impossible to factor*** $K = p \times q$ $\star\star\star\star\star$

4) Alice ***keeps secret*** her **Private Key** $= \boxed{\{\alpha\}}$

5) Since now $\boxed{\{\boldsymbol{Message}\}^{\beta\,\alpha} \bmod K = \{\boldsymbol{Message}\}}$ ...

[E] Bob sends Alice an **RSA-*encrypted*** message

$$\boxed{\text{Plain Text}} \xRightarrow[\text{digitize}]{} \left\{\boxed{\text{Plain Text}}\right\}^{\beta} \bmod K \equiv \boxed{\text{Cipher Text}}$$

[D] ... which Alice—and *only* Alice—can ***decrypt***:

$$\left\{\boxed{\text{Cipher Text}}\right\}^{\alpha} \bmod K = \boxed{\text{Plain Text}}\ !!!$$

How to *Attack* RSA Encryption?

Find an *EFFICIENT* algorithm to factor public key $K = p \times q$

$\exists$ algorithms to factor large numbers K, e.g., with $\boxed{N \equiv \log K}$ $\gg$ 128 bits?

storage size

¿ *Primitive*: Eve tries every $n = 2, 3, \ldots, \sqrt{K} \quad \Longrightarrow$

$$\tau_N = K^{1/2} = \exp\left[\tfrac{1}{2}\log K\right] = \exp\left[\tfrac{1}{2}N\right] \quad \text{steps}$$

which is *INEFFICIENT*!! $\Longleftrightarrow$ $\begin{cases} \tau_N \sim \mathcal{O}(K^a) \sim e^{aN} \sim e^{\#\,\texttt{digits}} \sim \#\,\texttt{values} \\ \tau_N > \mathcal{O}(\text{poly}[N]) \sim \text{poly}[\#\,\texttt{digits}] \end{cases}$

¿ Best for $N > 400$ bits is "Number Field Sieve":

$$\tau_N \sim K^{(\log\log K/\log K)^{2/3}} \sim \exp\left[N^{1/3}(\log N)^{2/3}\right]$$

which is *INEFFICIENT*!!

¿ Hmmm. Knowing $\{K{=}pq, \beta\}$ ***EFFICIENTLY*** implies $\{\alpha\}$ $\star$ .....

¿ Note that Eve ***does*** have the factors p & q of $K = p \times q$ in hand ***if*** she can solve this ***EFFICIENTLY*** for μ:

$$\boxed{\mu^2 \bmod K = 1}$$

because

$$(\mu+1)(\mu-1) \bmod (pq) = 0 \quad \Longrightarrow \quad (\mu+1)(\mu-1) = pq{\cdot}x = (py_1)(qy_2)$$

$$\Longrightarrow \begin{cases} \mu = +1 \bmod (pq) & = 1 & \text{(trivial)} \\ \mu = -1 \bmod (pq) & = pq - 1 & \text{(trivial)} \\ \mu = p{\cdot}y_1 - 1 \quad \& & \mu = q{\cdot}y_2 + 1 & \star \\ \mu = p{\cdot}y_1 + 1 \quad \& & \mu = q{\cdot}y_2 - 1 & \star \end{cases}$$

$\star \quad \Longrightarrow \quad \boxed{\gcd(\mu \pm 1, pq) = p} \quad \boxed{\gcd(\mu \mp 1, pq) = q}$

$\star$ Finding **g**reatest **c**ommon **d**ivisor via *Euclid's algorithm* ***is*** ***EFFICIENT***:

$$\tau_N \sim \log K = N \sim \mathcal{O}(\text{poly}[N]) \quad \text{steps}$$

¿ ..... **SO??** .....

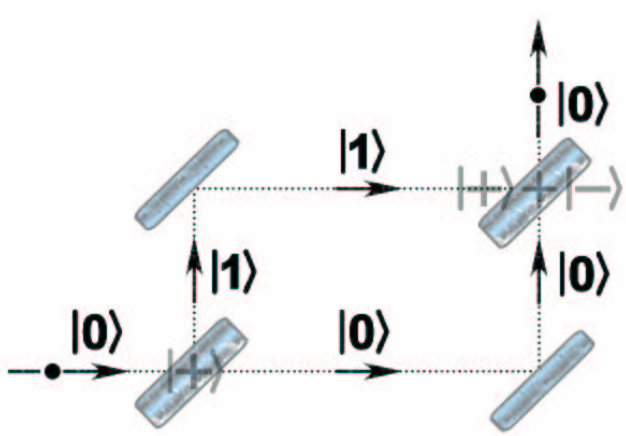
Qu[antum]bits

Bit $\boxed{\mathbf{b}}$	*vs.*	**Qubit** $\lvert\mathbf{q}\rangle$
$\begin{matrix}\boxed{\mathbf{0}}\\ \hline \boxed{\mathbf{1}}\end{matrix}$		$\left\{\begin{matrix}\lvert\mathbf{0}\rangle\\ \lvert\mathbf{1}\rangle\end{matrix}\right\}$
Store: $\boxed{\mathbf{b}} = \mathbf{0} \mid \mathbf{1}$		Store: $\lvert\mathbf{q}\rangle = \cos\vartheta\lvert\mathbf{0}\rangle + e^{i\varphi}\sin\vartheta\lvert\mathbf{1}\rangle$
—**2** possibilities		—∞ possibilities $(0 \le \vartheta, \varphi < 2\pi)$
Operation: SWITCH		Operation: UNITARY EVOLUTION
$\boxed{\mathbf{0}} \rightleftarrows \boxed{\mathbf{1}}$		$\lvert\mathbf{q}\rangle \longrightarrow \lvert\mathbf{q'}\rangle = \widehat{U}\lvert\mathbf{q}\rangle \longrightarrow \widehat{U}^{\dagger}\lvert\mathbf{q'}\rangle = \lvert\mathbf{q}\rangle$
Measure: only $\boxed{\mathbf{0}} \mid \boxed{\mathbf{1}}$		Measure: only $\lvert\mathbf{0}\rangle \mid \lvert\mathbf{1}\rangle$ ... or $\lvert\mathbf{0'}\rangle \mid \lvert\mathbf{1'}\rangle$
CLASSICAL		**SUPERPOSITION INTERFERENCE**

Single-qubit operations include "Hadamard transformation" $\widehat{U} = \widehat{H} = \widehat{U}^{\dagger}$

$$\left.\begin{aligned}\lvert\mathbf{0}\rangle \longrightarrow \widehat{H}\lvert\mathbf{0}\rangle \equiv \lvert+\rangle = \sqrt{\tfrac{1}{2}}\left(\lvert\mathbf{0}\rangle + \lvert\mathbf{1}\rangle\right)\\ \lvert\mathbf{1}\rangle \longrightarrow \widehat{H}\lvert\mathbf{1}\rangle \equiv \lvert-\rangle = \sqrt{\tfrac{1}{2}}\left(\lvert\mathbf{0}\rangle - \lvert\mathbf{1}\rangle\right)\end{aligned}\right\} \qquad \widehat{H} \doteq \begin{array}{c c} & \begin{array}{cc}\lvert\mathbf{0}\rangle & \lvert\mathbf{1}\rangle\end{array}\\ \begin{array}{c}\langle\mathbf{0}\rvert\\ \langle\mathbf{1}\rvert\end{array} & \begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\end{array}\Big/\sqrt{2}$$

which effectively **(i)** rotates a spinor about $\hat{\boldsymbol{y}}$ by 90°, or **(ii)** passes a spinor through a *half-silvered mirror* in, e.g., a *Mach-Zehnder Interferometer*:



Quantum Computation$_0$

Entangled Quantum State $|\Psi\rangle$ ***of two or more qubits*** $\equiv$

A coherent state in which it is impossible to assign a definite state to any one of its qubits.

—cf. quantum "non-locality," Bell's inequalities, EPR, ...

E.g., for 2 qubits: $$\boxed{|\Psi\rangle_{12} = \sqrt{\tfrac{1}{2}}\left[|0\rangle_1|1\rangle_2 + e^{i\varphi}|1\rangle_1|0\rangle_2\right]}$$

Quantum Computation on qubits $|\mathbf{q}\rangle_1|\mathbf{q}\rangle_2\cdots|\mathbf{q}\rangle_N$ is accomplished via

- ¿ *One-qubit* unitary transformations: $\ldots,\ \widehat{U}_i|\mathbf{q}\rangle_i,\ \ldots \quad (\mathbf{q} = \mathbf{0}|\mathbf{1})$
- ¿ *Two-qubit* unitary transformations: $\ldots,\ \widehat{U}_{i\neq j}|\mathbf{q}\rangle_i|\mathbf{q}\rangle_j,\ \ldots$
- ¿ *Multi-qubit* unitary transformations: $\widehat{U}\ \underbrace{|\mathbf{q}\rangle_{N-1}\cdots|\mathbf{q}\rangle_1|\mathbf{q}\rangle_0}_{\texttt{Register}}$

$\Longrightarrow$ **Exponential** gain in the capacity of information stored and in the efficiency of simultaneous information processing .....

1 0 1 0 1 0 1 0 1 0 1 0 1 0
0 1 0 1 0 1 0 1 0 1 0 1 0 1 Massively Parallel Computation 1 0 1 0 1 0 1 0 1 0 1 0 1 0
0 1 0 1 0 1 0 1 0 1 0 1 0 1

..... *BUT* ... only N qubits of data can be read/observed.

Nevertheless, the *effect* of all that information storage and processing on *a few* carefully chosen variables CAN be observed by exploiting ***entanglement***, allowing one to infer a *correct result* after n trials with

$$\boxed{\textbf{\textit{Probability}} \quad 1-\epsilon^n \underset{0<\epsilon<1}{\longrightarrow} \mathbf{1}^-}$$

Any computational algorithm can be implemented on a *Turing Machine*, or on a ***Quantum Turing Machine***.

But **Quantum Computation** does not expand what is POSSIBLE
— Only What is PRACTICAL.

One-qubit unitary transformations

Can be built up ***EFFICIENTLY*** to *arbitrary accuracy* $\epsilon \gtrsim 0$, in $\sim \mathcal{O}(1/\epsilon)$ steps, from a *finite basic set* of unitary transformations (in practice, ≥ 2).

E.g., employ ***Rabi flopping*** between the 2 states $\boxed{|\mathbf{0}\rangle \underset{\hbar\omega}{\longleftrightarrow} |\mathbf{1}\rangle}$

Jaynes-Cummings model ..... atom + microcavity photon field .....

$\{|\boldsymbol{g}, n\rangle, |\boldsymbol{e}, n{-}1\rangle\} \equiv \{|\mathbf{0}\rangle|\mathbf{n}\rangle_C, |\mathbf{1}\rangle|\mathbf{n{-}1}\rangle_C\}$ .....

LλA, RWA, near-resonance $\hbar\omega$ $\Longrightarrow$ t-evolution:

$$\begin{cases} |\boldsymbol{e}, n{-}1; t\rangle = \left[\cos\left(\frac{1}{2}\Omega_{n,\omega}t\right) + i\dfrac{\Delta_\omega}{\Omega_{n,\omega}}\sin\left(\frac{1}{2}\Omega_{n,\omega}t\right)\right]|\boldsymbol{e}, n{-}1\rangle \\ \qquad\qquad - \dfrac{\Omega_{\mathrm{R}n}}{\Omega_{n,\omega}}\, e^{+i\varphi}\sin\left(\frac{1}{2}\Omega_{n,\omega}t\right)|\boldsymbol{g}, n\rangle \\ |\boldsymbol{g}, n; t\rangle = \left[\cos\left(\frac{1}{2}\Omega_{n,\omega}t\right) - i\dfrac{\Delta_\omega}{\Omega_{n,\omega}}\sin\left(\frac{1}{2}\Omega_{n,\omega}t\right)\right]|\boldsymbol{g}, n\rangle \\ \qquad\qquad + \dfrac{\Omega_{\mathrm{R}n}}{\Omega_{n,\omega}}\, e^{-i\varphi}\sin\left(\frac{1}{2}\Omega_{n,\omega}t\right)|\boldsymbol{e}, n{-}1\rangle \end{cases}$$

Vacuum Rabi flopping freq.	$\Omega_{\mathrm{R}} \equiv \sqrt{8\pi\hbar\omega L^{-3}}\left\lvert q\,\langle\boldsymbol{g}\rvert\,\mathbf{r}\cdot\hat{\boldsymbol{\epsilon}}\,\lvert\boldsymbol{e}\rangle\right\rvert/\hbar\,,$	$\varphi \equiv \arg\,\langle\boldsymbol{g}\rvert\,\mathbf{r}\cdot\hat{\boldsymbol{\epsilon}}\,\lvert\boldsymbol{e}\rangle$ (POLARIZATION)
n-photon res. flopping freq.	$\Omega_{\mathrm{R}n} \equiv \sqrt{n}\,\Omega_{\mathrm{R}}$	
Detuning	$\Delta_\omega \equiv \omega - \omega_0\,,\quad \omega_0 \equiv (E_e - E_g)/\hbar$	
Dressed eigenfrequency	$\Omega_{n,\omega} \equiv \sqrt{{\Omega_{\mathrm{R}n}}^2 + {\Delta_\omega}^2} = \sqrt{n{\Omega_{\mathrm{R}}}^2 + (\omega - \omega_0)^2}$	

For $\Delta_\omega = 0$ & $n = 1$, on-resonance atom/single-photon–***entangling*** **pulses**:

$$\Omega_{\mathrm{R}n}t = \tfrac{1}{2}\cdot\pi \overset{\text{Split}}{\Longrightarrow} |\boldsymbol{e}, 0\rangle \underset{\pi/2}{\longrightarrow} \sqrt{\tfrac{1}{2}}\Big[|\boldsymbol{e}, 0\rangle - |\boldsymbol{g}, 1\rangle\Big]\,,\quad |\boldsymbol{g}, 1\rangle \underset{\pi/2}{\longrightarrow} \sqrt{\tfrac{1}{2}}\Big[|\boldsymbol{e}, 0\rangle + |\boldsymbol{g}, 1\rangle\Big]$$

$$\Omega_{\mathrm{R}n}t = 1\cdot\pi \overset{\text{Flip}}{\Longrightarrow} |\boldsymbol{e}, 0\rangle \underset{\pi}{\longrightarrow} -|\boldsymbol{g}, 1\rangle\,,\quad |\boldsymbol{g}, 1\rangle \underset{\pi}{\longrightarrow} +|\boldsymbol{e}, 0\rangle$$

$$\Omega_{\mathrm{R}n}t = 2\cdot\pi \overset{\text{Fermion}}{\Longrightarrow} |\boldsymbol{e}, 0\rangle \underset{2\pi}{\longrightarrow} -|\boldsymbol{e}, 0\rangle\,,\quad |\boldsymbol{g}, 1\rangle \underset{2\pi}{\longrightarrow} -|\boldsymbol{g}, 1\rangle$$

Quantum Computation$_2$ — Two Qubits — Entanglement!

Two-qubit unitary transformations

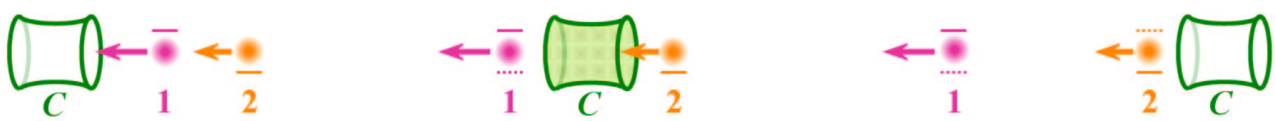
Can be built up ***EFFICIENTLY*** . . . ; e.g.,

$$\widehat{U}^{(\mathrm{CNOT})}_{i\neq j}\,|\mathbf{q}_i\rangle_i|\mathbf{q}_j\rangle_j = |\mathbf{q}_i\rangle_i|(\mathbf{q}_i+\mathbf{q}_j)\mathrm{mod}\,\mathbf{2}\rangle_j$$

C[ontrolled]**NOT** gate

CNOT	$\lvert 0\rangle_t$	$\lvert 1\rangle_c$
$\lvert 0\rangle_c$	$\lvert 0\rangle_c\lvert 0\rangle_t$	$\lvert 0\rangle_c\lvert 1\rangle_t$
$\lvert 1\rangle_c$	$\lvert 1\rangle_c\lvert 1\rangle_t$	$\lvert 1\rangle_c\lvert 0\rangle_t$

An EXAMPLE of ***entanglement*** . . . **of two qubits** via a cavity:



UNENTANGLED **CAVITY+** $|\mathbf{q}\rangle_1$ ***Entangled***

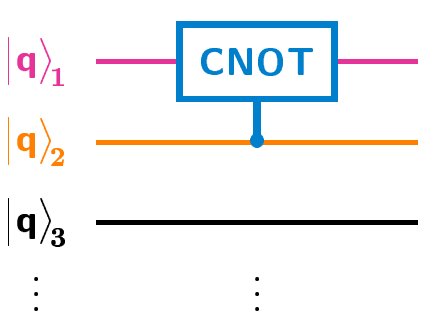
$$|\mathbf{1}\rangle_1|n{=}0\rangle_C|\mathbf{0}\rangle_2 \xRightarrow[(\pi/2)_1]{} \sqrt{\tfrac{1}{2}}\left[|\mathbf{1}\rangle_1|n{=}0\rangle_C|\mathbf{0}\rangle_2 - |\mathbf{0}\rangle_1|n{=}1\rangle_C|\mathbf{0}\rangle_2\right]$$

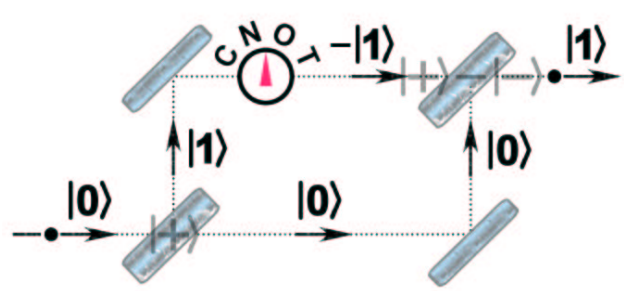
$|\mathbf{q}\rangle_1 + |\mathbf{q}\rangle_2$ ***Entangled***

$$\xRightarrow[(\pi)_2]{} \sqrt{\tfrac{1}{2}}\left[|\mathbf{1}\rangle_1|\mathbf{0}\rangle_2 - |\mathbf{0}\rangle_1|\mathbf{1}\rangle_2\right]|n{=}0\rangle_C$$

CNOT gate for 2-qubit states $|\mathbf{q}\rangle_{\mathrm{control}}\,|\mathbf{q}\rangle_{\mathrm{target}} \equiv |\mathbf{q}\,\mathbf{q}\rangle$:

$$\begin{array}{c} \\ \langle 0\,0| \\ \langle 0\,1| \\ \langle 1\,0| \\ \langle 1\,1| \end{array}
\begin{array}{c} \begin{array}{cccc} |0\,0\rangle & |0\,1\rangle & |1\,0\rangle & |1\,1\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \boxed{0} & \boxed{1} \\ 0 & 0 & \boxed{1} & \boxed{0} \end{pmatrix} \end{array}
= \frac{1}{2}\underbrace{\begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix}}_{(+\pi/2)_1}
\underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \boxed{-1} \end{pmatrix}}_{\text{IF } \mathbf{q}_1=\mathbf{q}_2=\mathbf{1}}
\underbrace{\begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix}}_{(-\pi/2)_1}$$





Quantum Computation$_3$ — Many Entangled Qubits

Multi-qubit **unitary transformations** $\widehat{U}_f$

Can ALWAYS be constructed ***EFFICIENTLY*** from 1- & 2-qubit ones .....

..... from 1-qubit pulses & **CNOT** gates!!

$\Longrightarrow$ ***Massively parallel computation*** — **exponential speedup**!

Prepare and operate on an N-qubit **INPUT** "***register***" in this initial state:

$$\left|\Psi_0\right\rangle = \widehat{H}_{N-1}\ldots\widehat{H}_1\widehat{H}_0\left|\mathbf{0}\right\rangle_{\boldsymbol{N-1}}\ldots\left|\mathbf{0}\right\rangle_{\mathbf{1}}\left|\mathbf{0}\right\rangle_{\mathbf{0}} = \prod_{i=0}^{N-1}\sqrt{\tfrac{1}{2}}\left(\left|\mathbf{0}\right\rangle_i + \left|\mathbf{1}\right\rangle_i\right)$$

$$= 2^{-N/2}\left[\left|\mathbf{0}\right\rangle_{\boldsymbol{N-1}}\ldots\left|\mathbf{0}\right\rangle_{\mathbf{1}}\left|\mathbf{0}\right\rangle_{\mathbf{0}} + \cdots\left\{\begin{matrix}\texttt{all } 2^{\texttt{N}}\texttt{ N-bit}\\ \texttt{binary ## x}\end{matrix}\right\}\cdots + \left|\mathbf{1}\right\rangle_{\boldsymbol{N-1}}\ldots\left|\mathbf{1}\right\rangle_{\mathbf{1}}\left|\mathbf{1}\right\rangle_{\mathbf{0}}\right]$$

$\Longrightarrow$ $\underline{\texttt{Computation f(x)}}$: $$\widehat{U}_f\left|\Psi_0\right\rangle = \frac{1}{\sqrt{2^N}}\,\widehat{U}_f\left(\sum_{\substack{\texttt{binary}\\ \texttt{x=0}}}^{2^{\texttt{N}}-1}\left|\texttt{x}\right\rangle\right) = \frac{1}{\sqrt{2^N}}\sum_{\substack{\texttt{binary}\\ \texttt{x=0}}}^{2^{\texttt{N}}-1}\left|\texttt{f(x)}\right\rangle$$

To get ***Entanglement*** between $\texttt{x}$ and $\texttt{f(x)}$, prepare also an N-qubit **OUTPUT** "***register***" in a reference state, e.g., $\left|\mathbf{0}\right\rangle = \left|\mathbf{0}\right\rangle_{\underline{\boldsymbol{N-1}}}\ldots\left|\mathbf{0}\right\rangle_{\underline{\mathbf{1}}}\left|\mathbf{0}\right\rangle_{\underline{\mathbf{0}}}$, now

$$\boxed{\widehat{U}_f\left|\Psi_0\right\rangle\left|\mathbf{0}\right\rangle = \frac{1}{\sqrt{2^N}}\,\widehat{U}_f\left(\sum_{\substack{\texttt{binary}\\ \texttt{x=0}}}^{2^{\texttt{N}}-1}\left|\texttt{x}\right\rangle\left|\mathbf{0}\right\rangle\right) = \frac{1}{\sqrt{2^N}}\sum_{\substack{\texttt{binary}\\ \texttt{x=0}}}^{2^{\texttt{N}}-1}\left|\texttt{x}\right\rangle\left|\texttt{f(x)}\right\rangle}$$

$$\widehat{U}_{\text{CNOT}}^{[N=2]}\,\frac{1}{2}\Big[\left|\mathbf{0}\right\rangle_{\mathbf{1}}\left|\mathbf{0}\right\rangle_{\mathbf{0}}\,\left|\mathbf{0}\right\rangle_{\underline{\mathbf{1}}}\left|\mathbf{0}\right\rangle_{\underline{\mathbf{0}}} + \left|\mathbf{0}\right\rangle_{\mathbf{1}}\left|\mathbf{1}\right\rangle_{\mathbf{0}}\,\left|\mathbf{0}\right\rangle_{\underline{\mathbf{1}}}\left|\mathbf{0}\right\rangle_{\underline{\mathbf{0}}} + \left|\mathbf{1}\right\rangle_{\mathbf{1}}\left|\mathbf{0}\right\rangle_{\mathbf{0}}\,\left|\mathbf{0}\right\rangle_{\underline{\mathbf{1}}}\left|\mathbf{0}\right\rangle_{\underline{\mathbf{0}}} + \left|\mathbf{1}\right\rangle_{\mathbf{1}}\left|\mathbf{1}\right\rangle_{\mathbf{0}}\,\left|\mathbf{0}\right\rangle_{\underline{\mathbf{1}}}\left|\mathbf{0}\right\rangle_{\underline{\mathbf{0}}}\Big]$$

$$= \frac{1}{2}\Big[\left|\mathbf{0}\right\rangle_{\mathbf{1}}\left|\mathbf{0}\right\rangle_{\mathbf{0}}\,\left|\mathbf{0}\right\rangle_{\underline{\mathbf{1}}}\left|\mathbf{0}\right\rangle_{\underline{\mathbf{0}}} + \left|\mathbf{0}\right\rangle_{\mathbf{1}}\left|\mathbf{1}\right\rangle_{\mathbf{0}}\,\left|\mathbf{0}\right\rangle_{\underline{\mathbf{1}}}\left|\mathbf{1}\right\rangle_{\underline{\mathbf{0}}} + \left|\mathbf{1}\right\rangle_{\mathbf{1}}\left|\mathbf{0}\right\rangle_{\mathbf{0}}\,\left|\mathbf{1}\right\rangle_{\underline{\mathbf{1}}}\left|\mathbf{1}\right\rangle_{\underline{\mathbf{0}}} + \left|\mathbf{1}\right\rangle_{\mathbf{1}}\left|\mathbf{1}\right\rangle_{\mathbf{0}}\,\left|\mathbf{1}\right\rangle_{\underline{\mathbf{1}}}\left|\mathbf{0}\right\rangle_{\underline{\mathbf{0}}}\Big]$$

$$= \widehat{U}_{\underline{\mathbf{10}}}^{(\text{CNOT})}\,\widehat{U}_{\mathbf{1}\underline{\mathbf{1}}}^{(\text{CNOT})}\,\widehat{U}_{\mathbf{0}\underline{\mathbf{0}}}^{(\text{CNOT})}\,\frac{1}{2}\Big[\left|\mathbf{0}\right\rangle\left|\mathbf{0}\right\rangle + \left|\mathbf{1}\right\rangle\left|\mathbf{0}\right\rangle + \left|\mathbf{2}\right\rangle\left|\mathbf{0}\right\rangle + \left|\mathbf{3}\right\rangle\left|\mathbf{0}\right\rangle\Big]$$

$$= \frac{1}{2}\Big[\left|\mathbf{0}\right\rangle\left|\mathbf{0}\right\rangle + \left|\mathbf{1}\right\rangle\left|\mathbf{1}\right\rangle + \left|\mathbf{2}\right\rangle\left|\mathbf{3}\right\rangle + \left|\mathbf{3}\right\rangle\left|\mathbf{2}\right\rangle\Big]$$

Quantum Factoring Algorithm of Peter Shor (1994)

0) *NB.*: To crack an **RSA**-encrypted message, solve $\boxed{\boldsymbol{\mu}^2 \bmod \boldsymbol{K} = \mathbf{1}}$.

If we can find any number y with $\mathbf{gcd}(y, \boldsymbol{K}) = \mathbf{1}$ and even period $\boldsymbol{r}$, then

$$\boxed{y^{\boldsymbol{r}} \bmod \boldsymbol{K} = \mathbf{1} \quad \Longrightarrow \quad \boldsymbol{\mu} = y^{\boldsymbol{r}/2} \bmod \boldsymbol{K}}$$

1) To factor $\boldsymbol{K}$ with $N \sim \log_2 2\boldsymbol{K}^2$, set an N-qubit register to initial state

$$\big|\Psi_0\big\rangle = \frac{1}{\sqrt{2^N}} \sum_{x=0}^{2^N-1} \big|x\big\rangle$$

and another N-qubit register to initial $\big|\mathbf{0}\big\rangle$ (all $\mathbf{0}$'s).

2) Pick a ***random*** number $y < \boldsymbol{K}$. Simultaneously— ***EFFICIENTLY*** — quantum-compute the numbers $f(x) = \{y^x \bmod \boldsymbol{K}\}$ in the 2nd register, thereby **entangling** them with the numbers $\{x\}$ in the 1st register:

$$\big|\Psi\big\rangle = \widehat{U}_f \big|\Psi_0\big\rangle\big|\mathbf{0}\big\rangle = \frac{1}{\sqrt{2^N}} \sum_{x=0}^{2^N-1} \big|x\big\rangle\big|f(x)\big\rangle = \frac{1}{\sqrt{2^N}} \sum_{x=0}^{2^N-1} \big|x\big\rangle\big|y^x \bmod \boldsymbol{K}\big\rangle$$

All results are here!! —— How to extract <u>periodicity</u> $\boldsymbol{r}$ of $y^x \bmod \boldsymbol{K}$**???**

3) We can at once find ALL numbers x that have some COMMON but ***random*** value $\boldsymbol{z} = y^{x_0+\lambda \boldsymbol{r}} \bmod \boldsymbol{K}$ by simply measuring 2nd register and finding whatever state $\big|\boldsymbol{z}\big\rangle$. This leaves 1st register in quasi-periodic superposition

$$\big|\psi_{x_0}\big\rangle = \frac{1}{\sqrt{L}} \sum_{\lambda=0}^{L \approx 2^N/\boldsymbol{r}} \big|x_0 + \lambda \boldsymbol{r}\big\rangle\,, \qquad 0 \le x_0 < \boldsymbol{r}\,.$$

We don't care about the shift x_0 —only the periodicity $\boldsymbol{r}$, so ...

4) $\star\star\star$ Compute Discrete $\boxed{[\mathcal{F}\text{ast}]\ \mathcal{F}\text{ourier}\ \mathcal{T}\text{ransform of } \big|\psi_{x_0}\big\rangle}$ $\star\star\star$

Quantum $\mathcal{FFT}$ is ***EFFICIENT*** —involves 1-qubit $\widehat{H}$'s and 2-qubit rephasing transformations, yields: $\mathcal{FFT}\big|\psi_{x_0}\big\rangle = \frac{1}{\sqrt{\boldsymbol{r}}} \sum_{j=0}^{\boldsymbol{r}-1} e^{2\pi i x_0 j/\boldsymbol{r}} \big|j\,(2^N/\boldsymbol{r})\big\rangle$

5) By repeating above measurements n times, $\mathcal{FFT}$ converges to invariant even period $\boldsymbol{r}$ of some y with probability $\gtrsim \mathcal{O}([1/2N]^n)$.

An Example of Factoring via Shor's Algorithm

0) FOR EXAMPLE, let $p = 5$ & $q = 7$, solve $\boxed{\mu^2 \bmod 35 = 1}$.

If we can find any number y with $\mathbf{gcd}(y, 35) = 1$ and even period r, then

$$\boxed{y^r \bmod 35 = 1 \quad \Longrightarrow \quad \mu = y^{r/2} \bmod 35}$$

1) To factor 35 with $N = 11$ $(2^{11-1=2047})$, set 11-qubit registers to initial

$$|\Psi_0\rangle|0\rangle = \frac{1}{\sqrt{2^N}} \sum_{\substack{\text{binary} \\ x=0}}^{2047} |x\rangle\,|0\rangle$$

2) Pick a ***random*** number $y < 35$. Simultaneously— ***EFFICIENTLY*** — quantum-compute the numbers $\{f(x) = y^x \bmod 35\}$ $(x=0,\ldots,2047)$, thereby **entangling** INPUT and OUTPUT registers:

$$|\Psi\rangle = \widehat{U}_f|\Psi_0\rangle|0\rangle = \frac{1}{\sqrt{2^N}} \sum_{x=0}^{2047} |x\rangle|f(x)\rangle = \frac{1}{\sqrt{2^N}} \sum_{x=0}^{2047} |x\rangle|y^x \bmod 35\rangle$$

E.g., for $\boxed{y = 9}$ (which has periodicity $r = 6$):

$$\begin{aligned}|\Psi\rangle \propto\ & |0\rangle|1\rangle + |1\rangle|9\rangle + |2\rangle|11\rangle + |3\rangle|29\rangle + |4\rangle|16\rangle + |5\rangle|4\rangle \\ & + |6\rangle|1\rangle + |7\rangle|9\rangle + |8\rangle|11\rangle + |9\rangle|29\rangle + \cdots + |2046\rangle|1\rangle + |2047\rangle|9\rangle\end{aligned}$$

3) Measure ***random*** $|z\rangle$ of OUTPUT register (random $z = y^x \bmod 35$), leaves INPUT register in a quasi-periodic superposition of $\{|x\rangle\}$ with $x = x_0 + \lambda r$; e.g., a measurement of $\boxed{|z\rangle = |11\rangle}$ leaves $x_0 = 2$, $(\lambda=0,\ldots,340)$:

$$|\psi_{x_0=2}\rangle \propto |2\rangle + |8\rangle + |14\rangle + |20\rangle + \cdots + |2036\rangle + |2042\rangle$$

4)

$$\boxed{\begin{aligned}\mathcal{FFT}\,|\psi_{x_0=2}\rangle = \frac{1}{\sqrt{6..}} \Big[& |0\rangle + e^{1\cdot 2\pi i x_0/6}|340\rangle + e^{2\cdot 2\pi i x_0/6}|680\rangle \\ & + e^{3\cdot 2\pi i x_0/6}|1020\rangle + e^{4\cdot 2\pi i x_0/6}|1360\rangle + e^{5\cdot 2\pi i x_0/6}|1700\rangle + e^{6\cdot 2\pi i x_0 i/6}|2040\rangle\Big]\end{aligned}}$$

5) Repeated measurement of this state (*any* $0 \le x_0 \lesssim r$) determines

$\boxed{r = 6} \quad \Longrightarrow \quad \mu = y^{r/2} \bmod 35 = 9^3 \bmod 35 = \boxed{29 = \mu} \quad \Longrightarrow \quad p = 5,\ q = 7$

Alice & Bob & Eve Redux