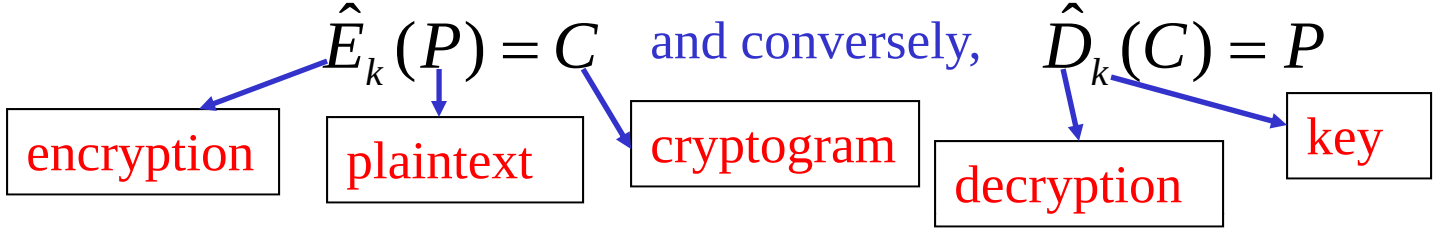
Quantum Cryptography

1. Quantum key distribution with entangled states

Key: a set of specific parameters supplied together with the plaintext (cryptogram) as a input to the encrypting (decrypting) algorithm.



E and *D*: publicly known; cryptogram security: key !!!

Example) Digital alphabet $C = (P + k) \pmod{30}$

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	Q	X	Y	Z		?	,	.
20	21	22	23	24	25	26	27	28	29

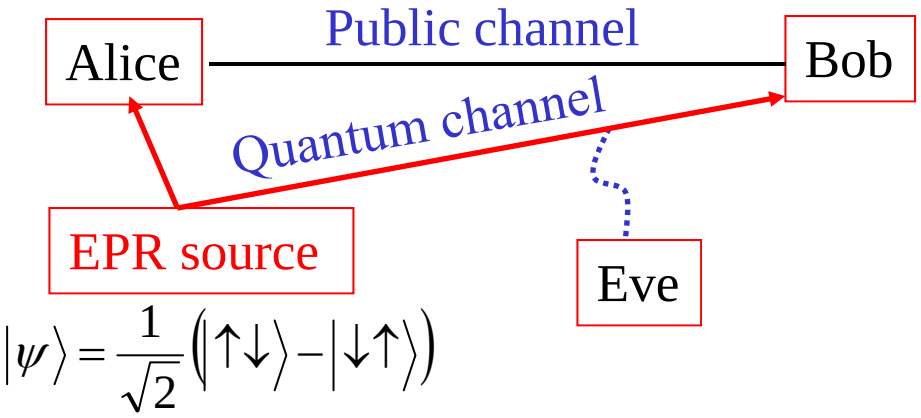
Alphabet	Q
P	16
k	16
C	2
cryptogram	C

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	Q	X	Y	Z		?	,	.
20	21	22	23	24	25	26	27	28	29

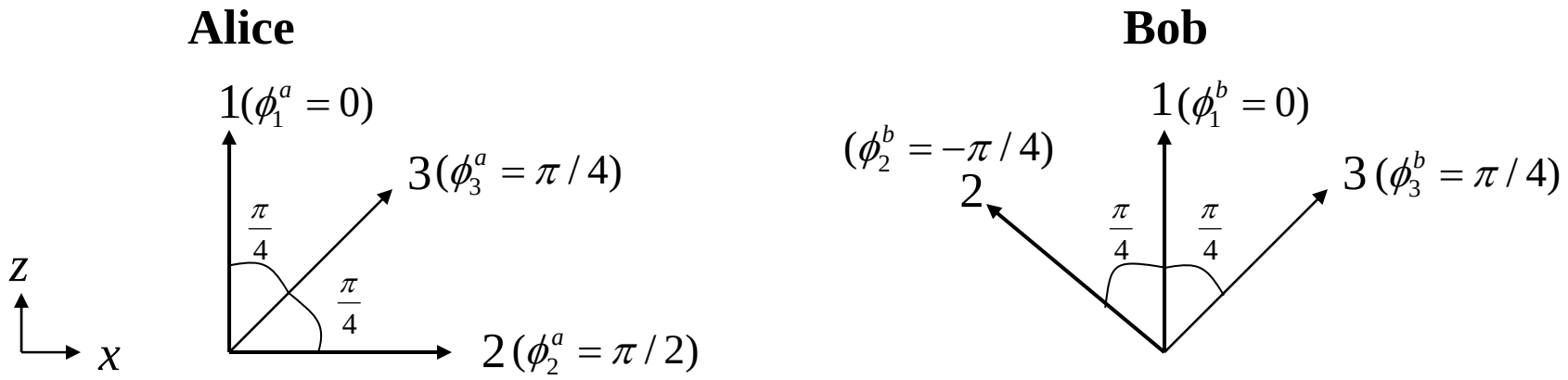
Q. Find the cryptogram of the word " QUANTUM ".

Plain text	Q	U	A	N	T	U	M
Alphabet number (P)	16	20	0	13	19	20	12
Key (k)	16	5	28	14	26	9	21
Encrypted alphabet number (C)	2	25	28	27	15	29	3
cryptogram	C	Z	,	?	P	.	D

Transmission of the raw key



Alice and Bob choose their bases randomly and independently for each pair of incoming particles.



Correlation coefficient

$$E\left(\phi_i^a, \phi_j^b\right) = P_{++}\left(\phi_i^a, \phi_j^b\right) + P_{--}\left(\phi_i^a, \phi_j^b\right) - P_{+-}\left(\phi_i^a, \phi_j^b\right) - P_{-+}\left(\phi_i^a, \phi_j^b\right)$$

Where $P_{\pm\pm}\left(\phi_i^a, \phi_j^b\right)$ denotes the probability of the particle 1 and 2 spin states defined by ϕ_i^a and ϕ_j^b.

$$P_{++}\left(\phi_i^a, \phi_j^b\right) = \frac{1}{2}\sin^2\frac{\phi_i^a - \phi_j^b}{2} \qquad P_{--}\left(\phi_i^a, \phi_j^b\right) = \frac{1}{2}\sin^2\frac{\phi_i^a - \phi_j^b}{2}$$

$$P_{+-}\left(\phi_i^a, \phi_j^b\right) = \frac{1}{2}\cos^2\frac{\phi_i^a - \phi_j^b}{2} \qquad P_{-+}\left(\phi_i^a, \phi_j^b\right) = \frac{1}{2}\cos^2\frac{\phi_i^a - \phi_j^b}{2}$$

$$\Rightarrow E\left(\phi_i^a, \phi_j^b\right) = \sin^2\frac{\phi_i^a - \phi_j^b}{2} - \cos^2\frac{\phi_i^a - \phi_j^b}{2} = -\cos\left(\phi_i^a - \phi_j^b\right)$$

Alice and Bob using analyzers of the same orientation,

$$E\left(\phi_1^a, \phi_1^b\right) = E\left(\phi_3^a, \phi_3^b\right) = -1$$

Alice and Bob using analyzers of different orientations,

$$S = E\left(\phi_1^a, \phi_3^b\right) + E\left(\phi_1^a, \phi_2^b\right) + E\left(\phi_2^a, \phi_3^b\right) - E\left(\phi_2^a, \phi_2^b\right) = -2\sqrt{2}$$

Measurement	1	2	3	4	5	6	…
Alice	ϕ_1^a	ϕ_2^a	ϕ_3^a	ϕ_2^a	ϕ_1^a	ϕ_1^a	…
Bob	ϕ_3^b	ϕ_2^b	ϕ_3^b	ϕ_3^b	ϕ_1^b	ϕ_2^b	…
Group	T	T	K	T	K	T	…

Group (T) : different orientation of the analyzers
Group (K): same orientation of the analyzers

Alice and Bob reveal publicly the results of the group (T).
$\Rightarrow$ This allows them to establish the value of *S*.

w/o Eve : $S = -2\sqrt{2}$

With Eve: $S \neq -2\sqrt{2}$