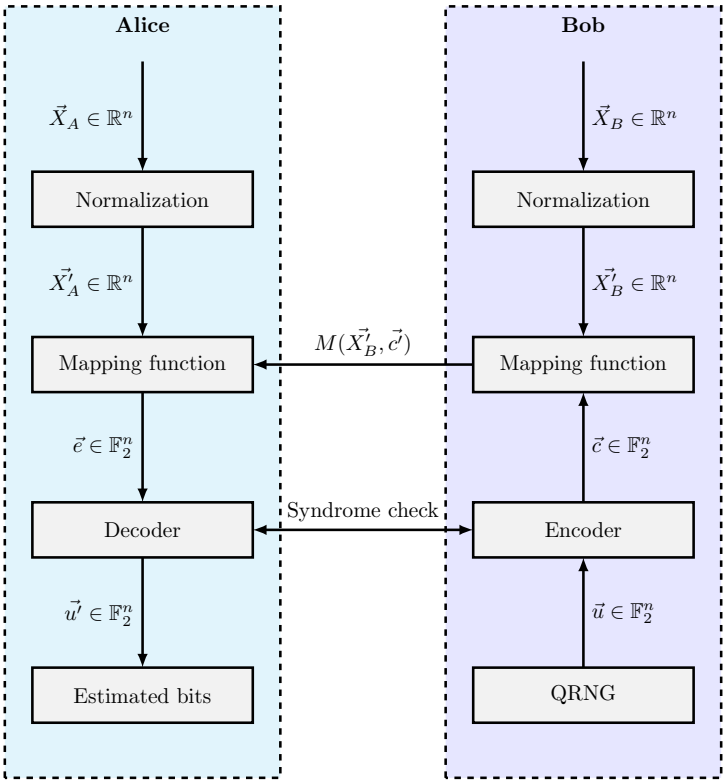
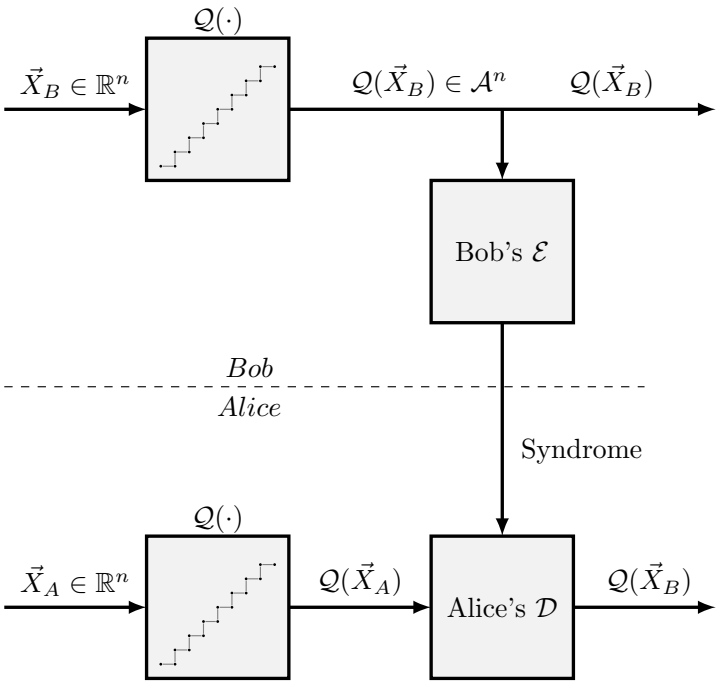
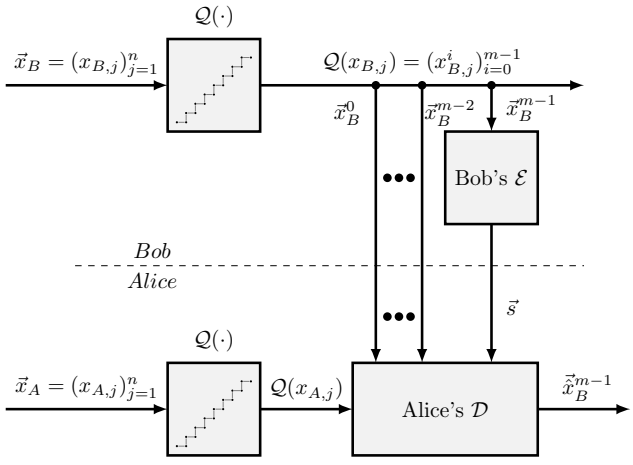
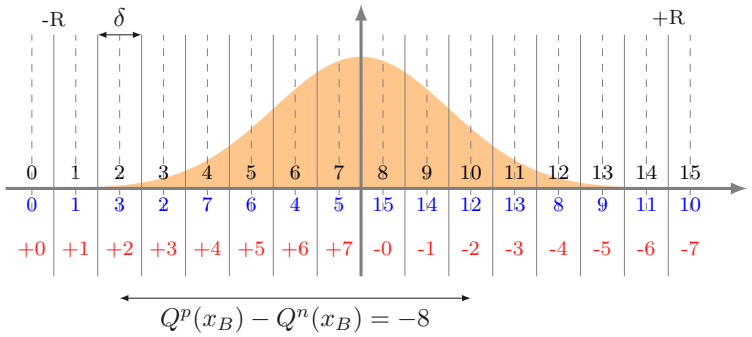
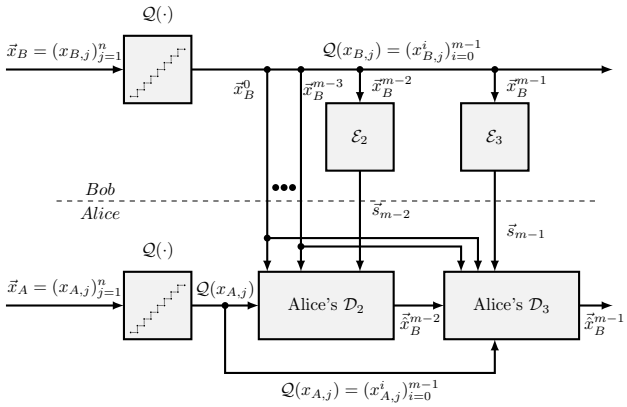
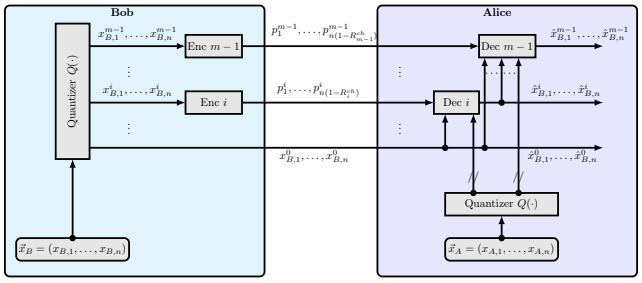

Alice
Bob
$\vec{X}_A \in \mathbb{R}^n$
$\vec{X}_B \in \mathbb{R}^n$
Normalization
Normalization
$\vec{X'}_A \in \mathbb{R}^n$
$\vec{X'}_B \in \mathbb{R}^n$
$M(\vec{X'}_B, \vec{c'})$
Mapping function
Mapping function
$\vec{e} \in \mathbb{F}_2^n$
$\vec{c} \in \mathbb{F}_2^n$
Syndrome check
Decoder
Encoder
$\vec{u'} \in \mathbb{F}_2^n$
$\vec{u} \in \mathbb{F}_2^n$
Estimated bits
QRNG

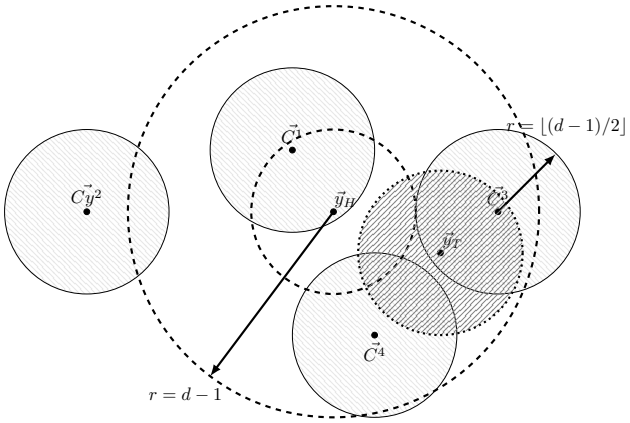

$\mathcal{Q}(\cdot)$
$\vec{X}_B \in \mathbb{R}^n$
$\mathcal{Q}(\vec{X}_B) \in \mathcal{A}^n$
$\mathcal{Q}(\vec{X}_B)$
Bob's $\mathcal{E}$
Bob
Alice
Syndrome
$\mathcal{Q}(\cdot)$
$\vec{X}_A \in \mathbb{R}^n$
$\mathcal{Q}(\vec{X}_A)$
Alice's $\mathcal{D}$
$\mathcal{Q}(\vec{X}_B)$

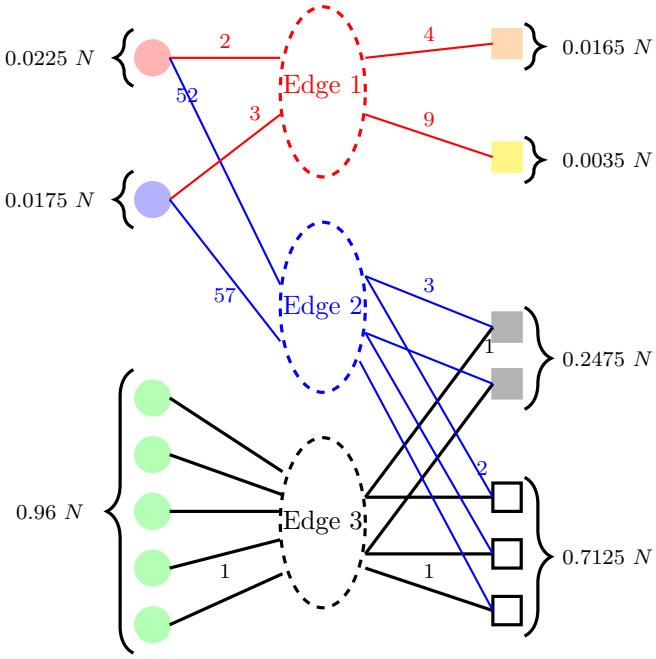

$\mathcal{Q}(\cdot)$
$\vec{x}_B = (x_{B,j})_{j=1}^n$
$\mathcal{Q}(x_{B,j}) = (x_{B,j}^i)_{i=0}^{m-1}$
$\vec{x}_B^0$
$\vec{x}_B^{m-2}$
$\vec{x}_B^{m-1}$
Bob's $\mathcal{E}$
Bob
Alice
$\vec{s}$
$\mathcal{Q}(\cdot)$
$\vec{x}_A = (x_{A,j})_{j=1}^n$
$\mathcal{Q}(x_{A,j})$
Alice's $\mathcal{D}$
$\vec{x}_B^{m-1}$

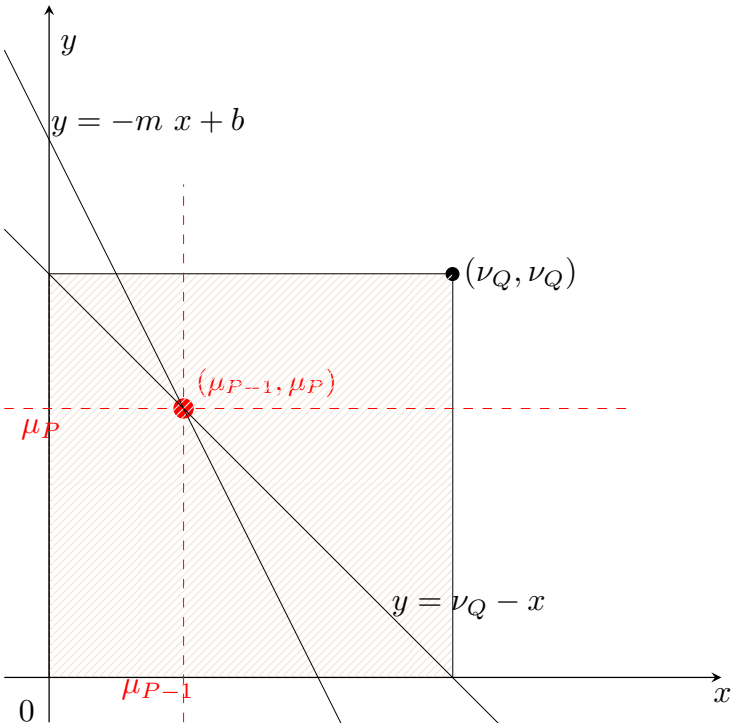

-R
δ
+R
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
0 1 3 2 7 6 4 5 15 14 12 13 8 9 11 10
+0 +1 +2 +3 +4 +5 +6 +7 -0 -1 -2 -3 -4 -5 -6 -7
$Q^p(x_B) - Q^n(x_B) = -8$

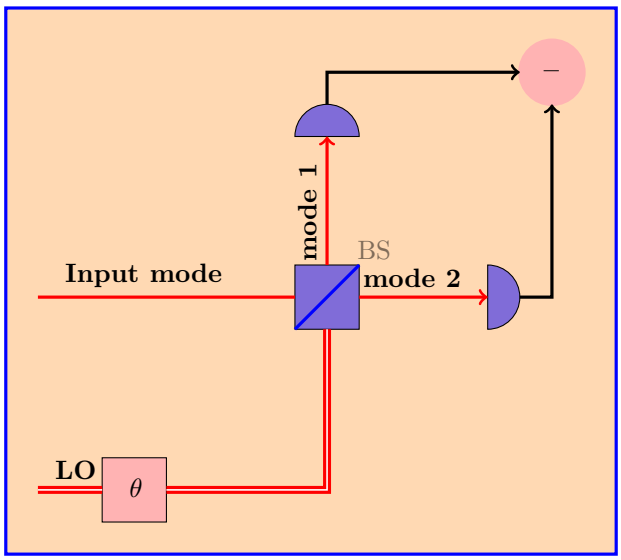

$\mathcal{Q}(\cdot)$
$\vec{x}_B = (x_{B,j})_{j=1}^n$
$\mathcal{Q}(x_{B,j}) = (x_{B,j}^i)_{i=0}^{m-1}$
$\vec{x}_B^0$
$\vec{x}_B^{m-3}$
$\vec{x}_B^{m-2}$
$\vec{x}_B^{m-1}$
$\mathcal{E}_2$
$\mathcal{E}_3$
Bob
Alice
$\vec{s}_{m-2}$
$\vec{s}_{m-1}$
$\mathcal{Q}(\cdot)$
$\vec{x}_A = (x_{A,j})_{j=1}^n$
$\mathcal{Q}(x_{A,j})$
Alice's $\mathcal{D}_2$
Alice's $\mathcal{D}_3$
$\hat{\vec{x}}_B^{m-2}$
$\hat{\vec{x}}_B^{m-1}$
$\mathcal{Q}(x_{A,j}) = (x_{A,j}^i)_{i=0}^{m-1}$

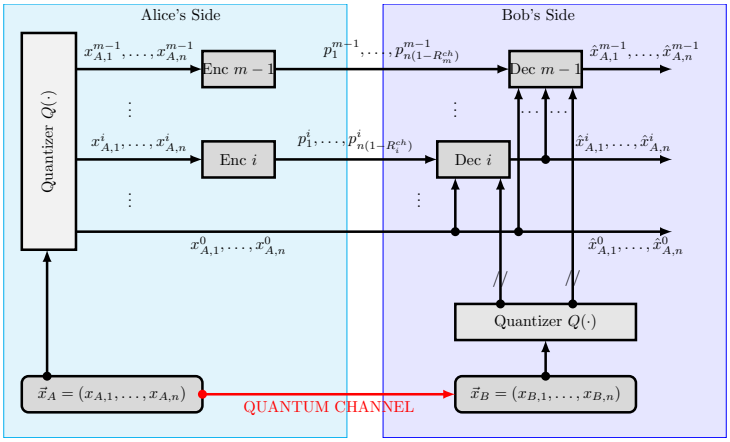

Bob
Alice
Quantizer $Q(\cdot)$
Enc $m-1$
Enc i
Dec $m-1$
Dec i
Quantizer $Q(\cdot)$
$\vec{x}_B = (x_{B,1}, \ldots, x_{B,n})$
$\vec{x}_A = (x_{A,1}, \ldots, x_{A,n})$

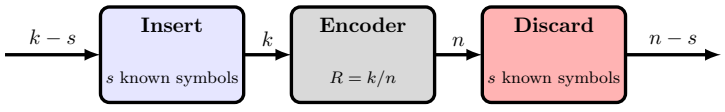

$\vec{C^1}$
$\vec{C^2}$
$\vec{C^3}$
$\vec{C^4}$
$\vec{y}_H$
$\vec{y}_T$
$r = \lfloor (d-1)/2 \rfloor$
$r = d - 1$

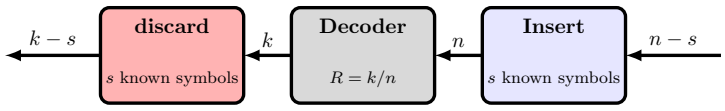

0.0225 N
0.0175 N
0.96 N
0.0165 N
0.0035 N
0.2475 N
0.7125 N
Edge 1
Edge 2
Edge 3
2
52
3
4
9
57
3
1
2
1
1

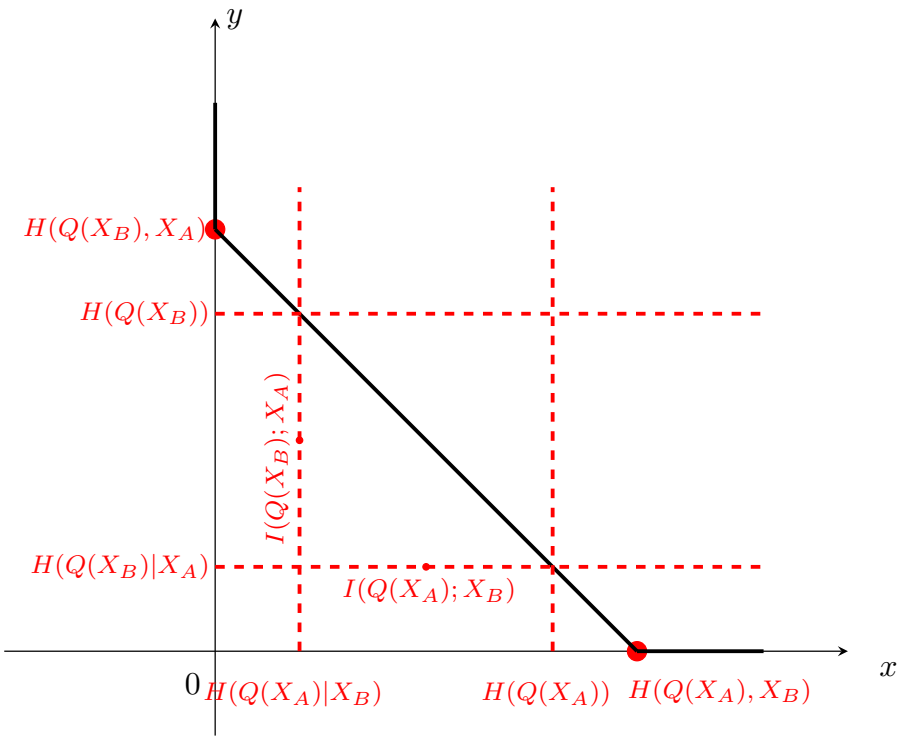

y
$y = -m\ x + b$
(ν_Q, ν_Q)
(μ_{P-1}, μ_P)
μ_P
$y = \nu_Q - x$
μ_{P-1}
0
x

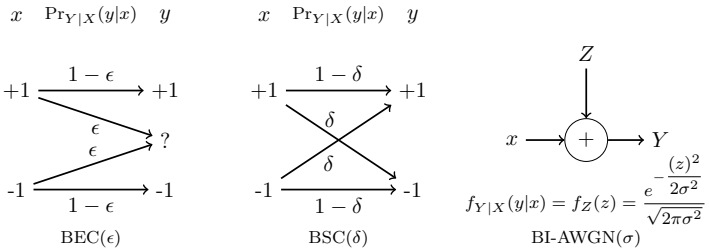

−
mode 1
BS
Input mode
mode 2
LO
θ


Alice's Side
Bob's Side
Quantizer $Q(\cdot)$
Enc $m-1$
Enc i
Dec $m-1$
Dec i
$x^{m-1}_{A,1},\ldots,x^{m-1}_{A,n}$
$p^{m+1}_1,\ldots,p^{m-1}_{n(1-R^{ch}_m)}$
$\hat{x}^{m-1}_{A,1},\ldots,\hat{x}^{m-1}_{A,n}$
$x^i_{A,1},\ldots,x^i_{A,n}$
$p^i_1,\ldots,p^i_{n(1-R^{ch}_i)}$
$\hat{x}^i_{A,1},\ldots,\hat{x}^i_{A,n}$
$x^0_{A,1},\ldots,x^0_{A,n}$
$\hat{x}^0_{A,1},\ldots,\hat{x}^0_{A,n}$
Quantizer $Q(\cdot)$
$\vec{x}_A=(x_{A,1},\ldots,x_{A,n})$
QUANTUM CHANNEL
$\vec{x}_B=(x_{B,1},\ldots,x_{B,n})$


$k-s$
Insert
s known symbols
k
Encoder
$R=k/n$
n
Discard
s known symbols
$n-s$


$k-s$
discard
s known symbols
k
Decoder
$R=k/n$
n
Insert
s known symbols
$n-s$


y
$H(Q(X_B), X_A)$
$H(Q(X_B))$
$I(Q(X_B); X_A)$
$H(Q(X_B)|X_A)$
$I(Q(X_A); X_B)$
0
$H(Q(X_A)|X_B)$
$H(Q(X_A))$
$H(Q(X_A), X_B)$
x


x $\Pr_{Y|X}(y|x)$ y
+1
$1-\epsilon$
+1
ϵ
?
ϵ
-1
-1
$1-\epsilon$
BEC(ϵ)
x $\Pr_{Y|X}(y|x)$ y
+1
$1-\delta$
+1
δ
δ
-1
-1
$1-\delta$
BSC(δ)
Z
x
+
Y
$f_{Y|X}(y|x) = f_Z(z) = \frac{e^{-\frac{(z)^2}{2\sigma^2}}}{\sqrt{2\pi\sigma^2}}$
BI-AWGN(σ)

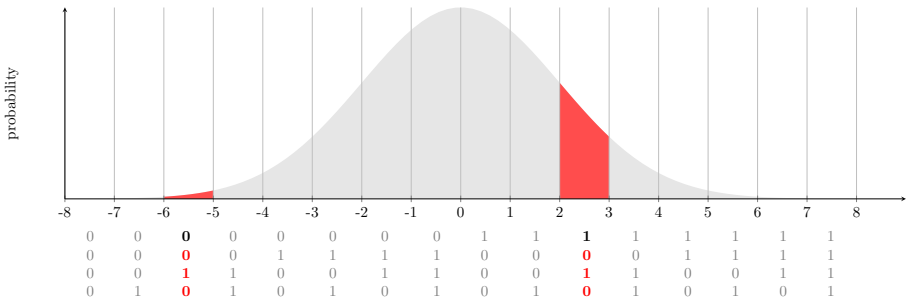


Figure 1: (Color online) The binary outputs of a 4-level quantizer. The top row denotes the most significant bits and the lowest row represents the least significant bit. Individually each row can be considered as a source with equiprobable binary outputs. But knowing the correct values of low significant bits give information about the most significant bit.