Fading wiretap channel with no CSI anywhere

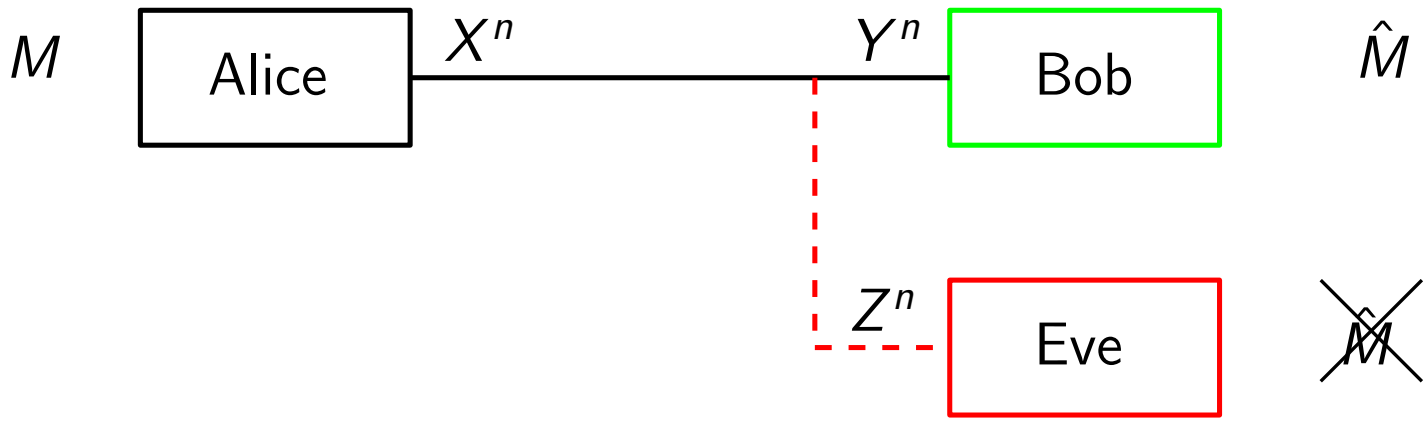
Pritam Mukherjee, Şennur Ulukuş

University of Maryland, College Park

ISIT, 2013

The Wiretap channel

- Introduced by Wyner in 1975

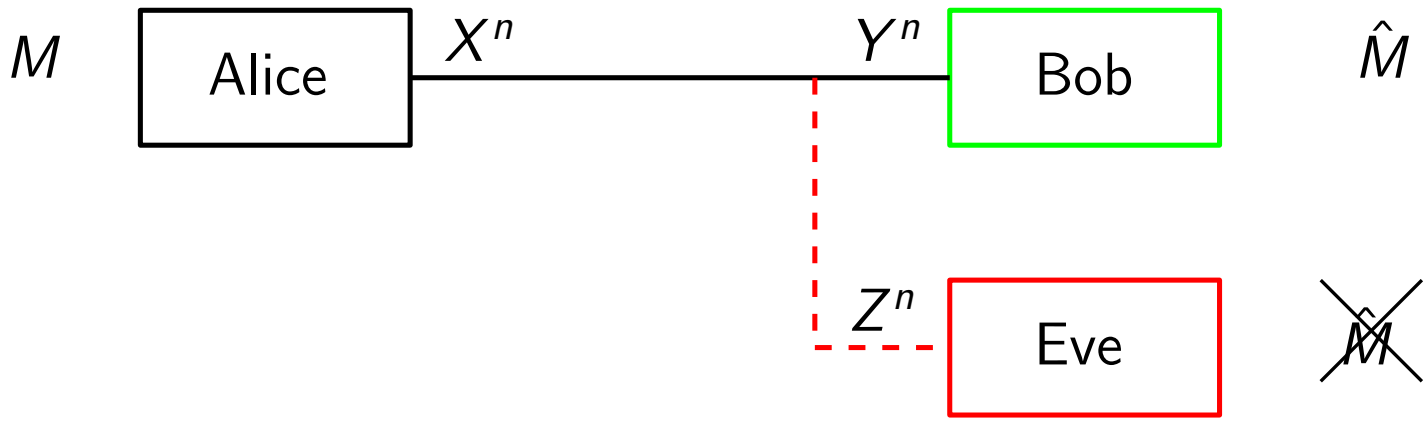


$$\text{Reliability: } \mathbb{P}(\hat{M} \neq M) \leq \epsilon$$

$$\text{Security: } \frac{1}{n} I(M; Z^n) \leq \epsilon$$

The Wiretap channel

- Introduced by Wyner in 1975



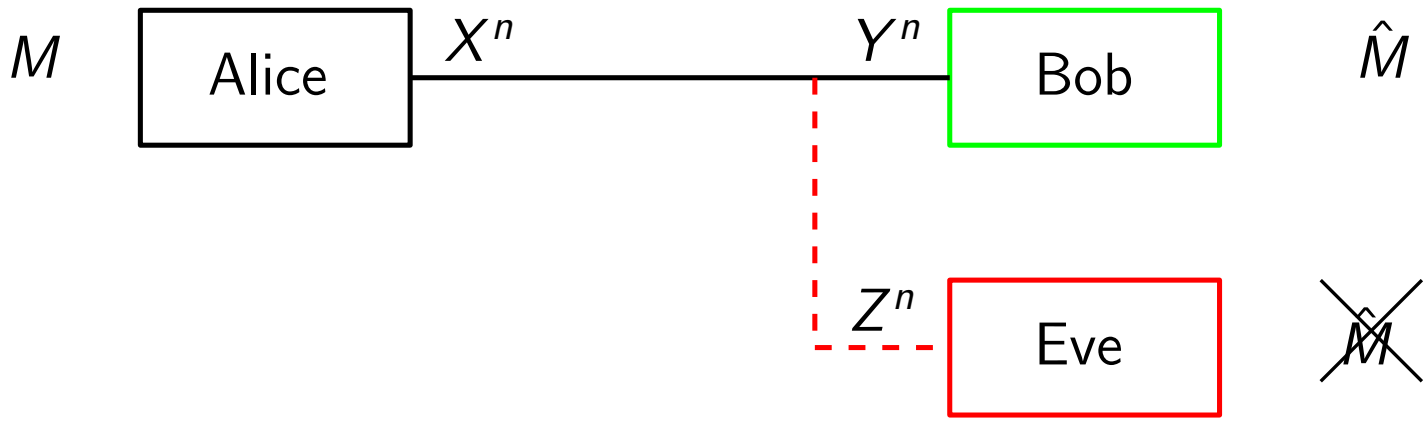
$$\text{Reliability: } \mathbb{P}(\hat{M} \neq M) \leq \epsilon$$

$$\text{Security: } \frac{1}{n} I(M; Z^n) \leq \epsilon$$

- **Key assumption**: DMC with $X \to Y \to Z$ (*degradedness*).

The Wiretap channel

- Introduced by Wyner in 1975



$$\text{Reliability: } \mathbb{P}(\hat{M} \neq M) \leq \epsilon$$

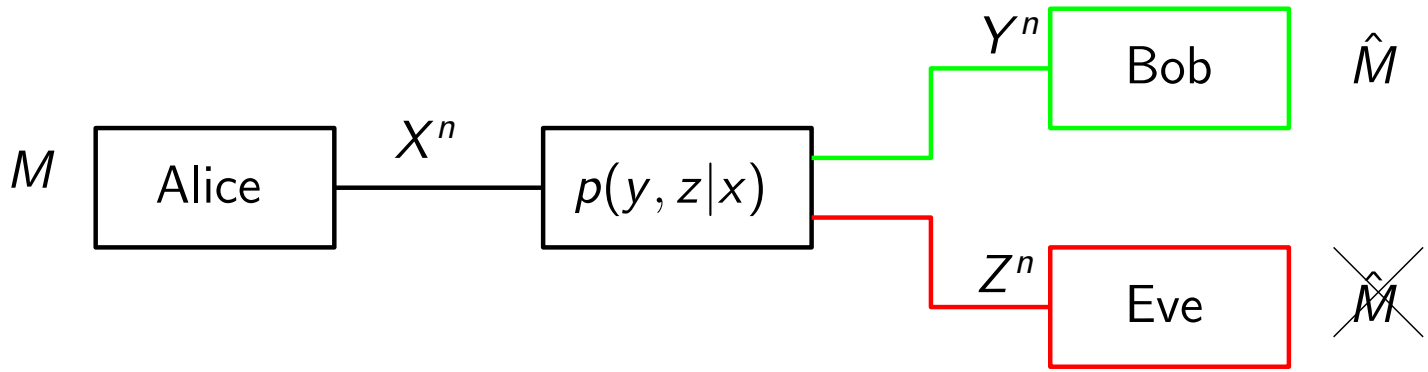
$$\text{Security: } \frac{1}{n} I(M; Z^n) \leq \epsilon$$

- **Key assumption**: DMC with $X \to Y \to Z$ (*degradedness*).
- *Secrecy capacity* given by,

$$C_s = \max_{p(x)} I(X; Y) - I(X; Z)$$

General wiretap channel

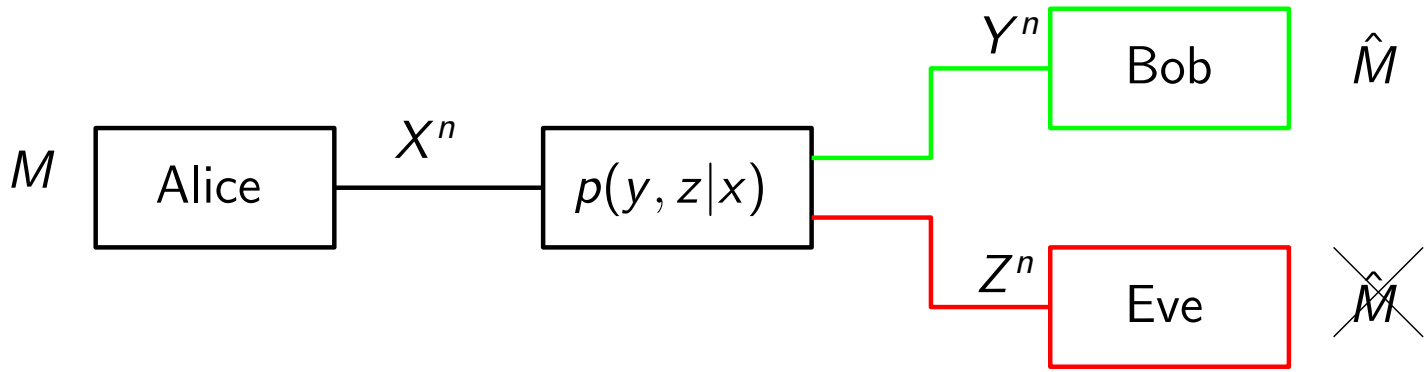
- Csiszár and Körner in 1978.



- **No** *degradedness* and generalizes to arbitrary alphabets.

General wiretap channel

- Csiszár and Körner in 1978.

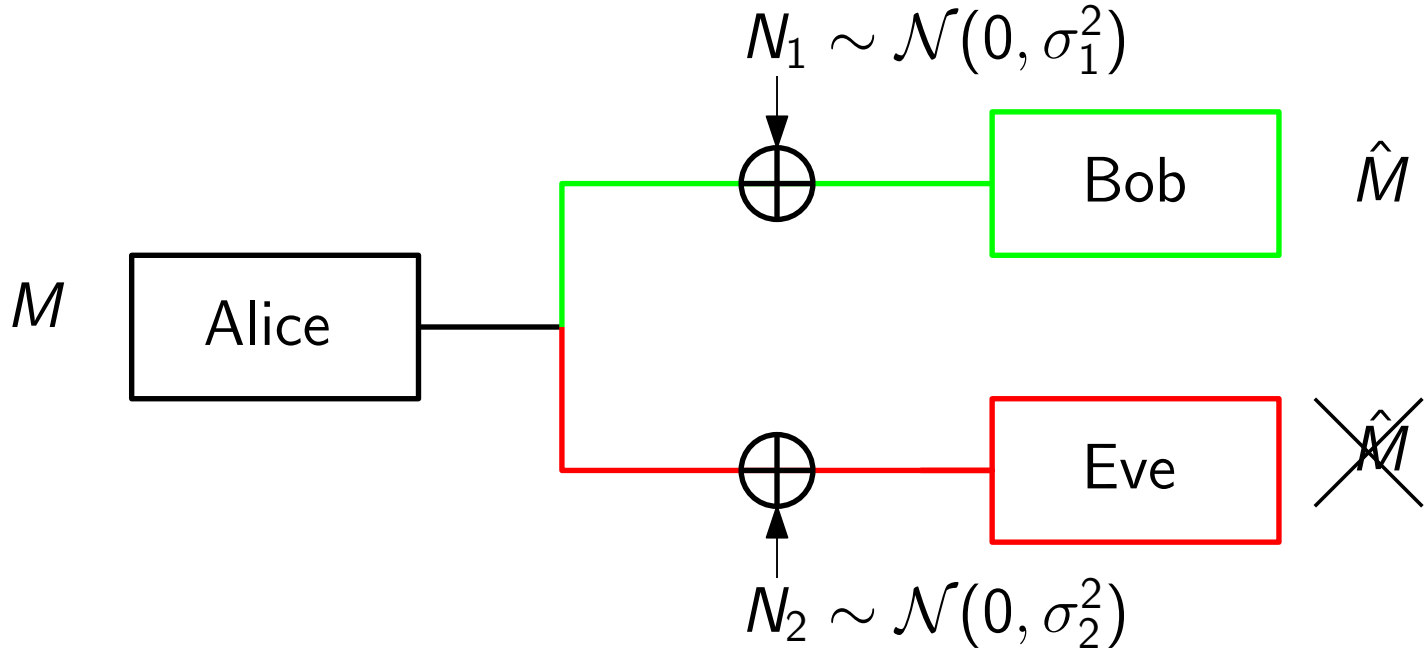


- **No** *degradedness* and generalizes to arbitrary alphabets.
- *Secrecy capacity* given by,

$$C_s = \max_{V \to X \to Y,Z} I(V;Y) - I(V;Z)$$

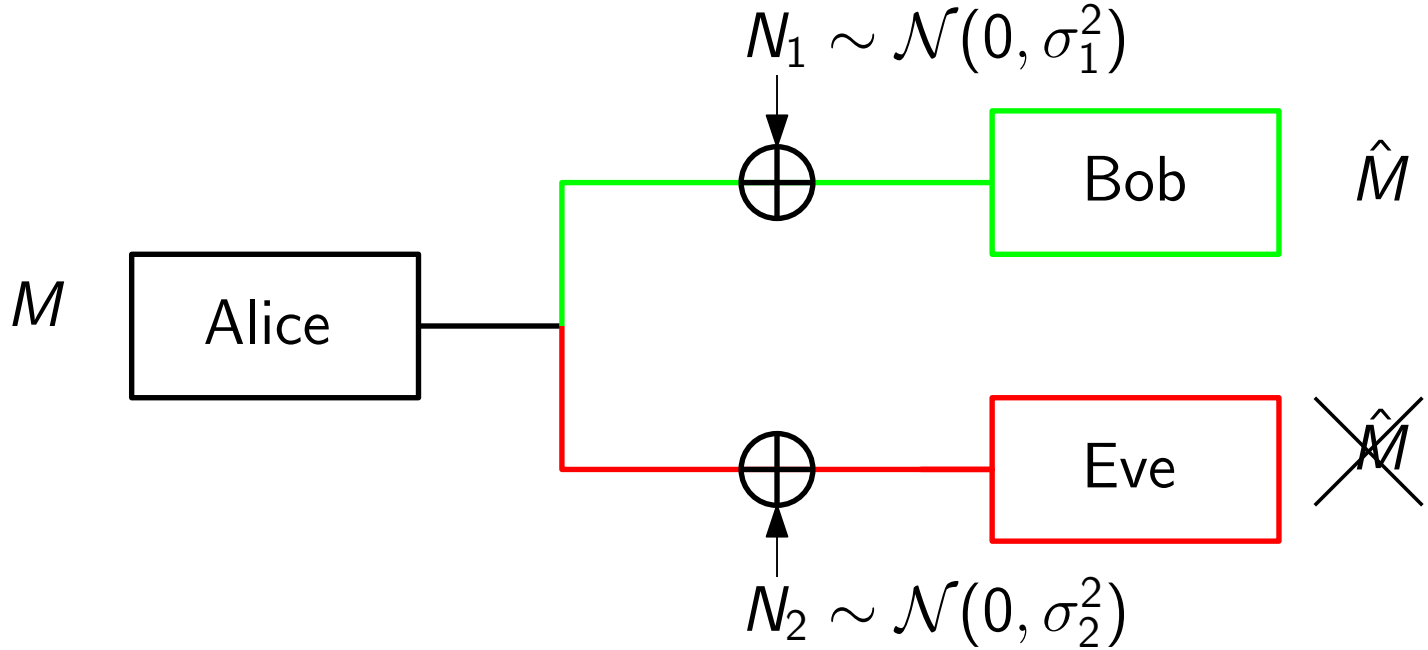
The Gaussian wiretap channel

- Leung-Yan-Cheong and Hellman in 1978.



The Gaussian wiretap channel

- Leung-Yan-Cheong and Hellman in 1978.

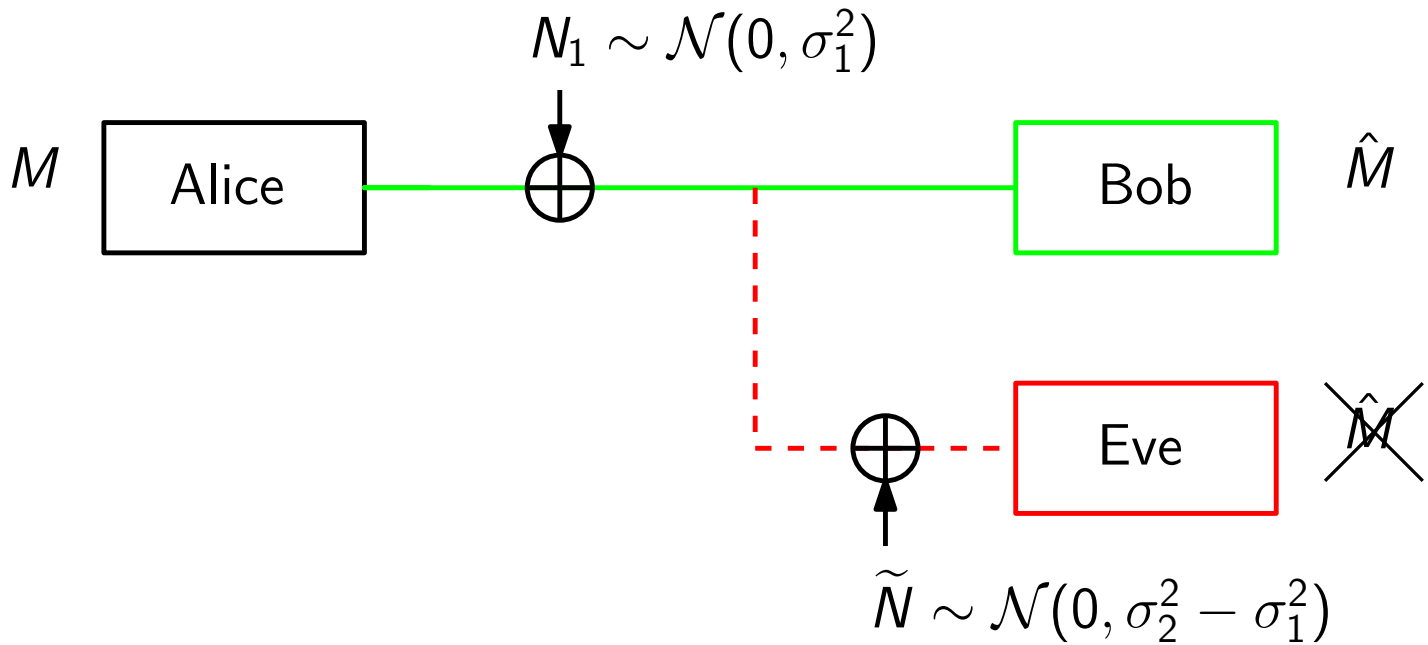


- *Secrecy capacity* is given by,

$$C_s = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\sigma_2^2}\right)$$

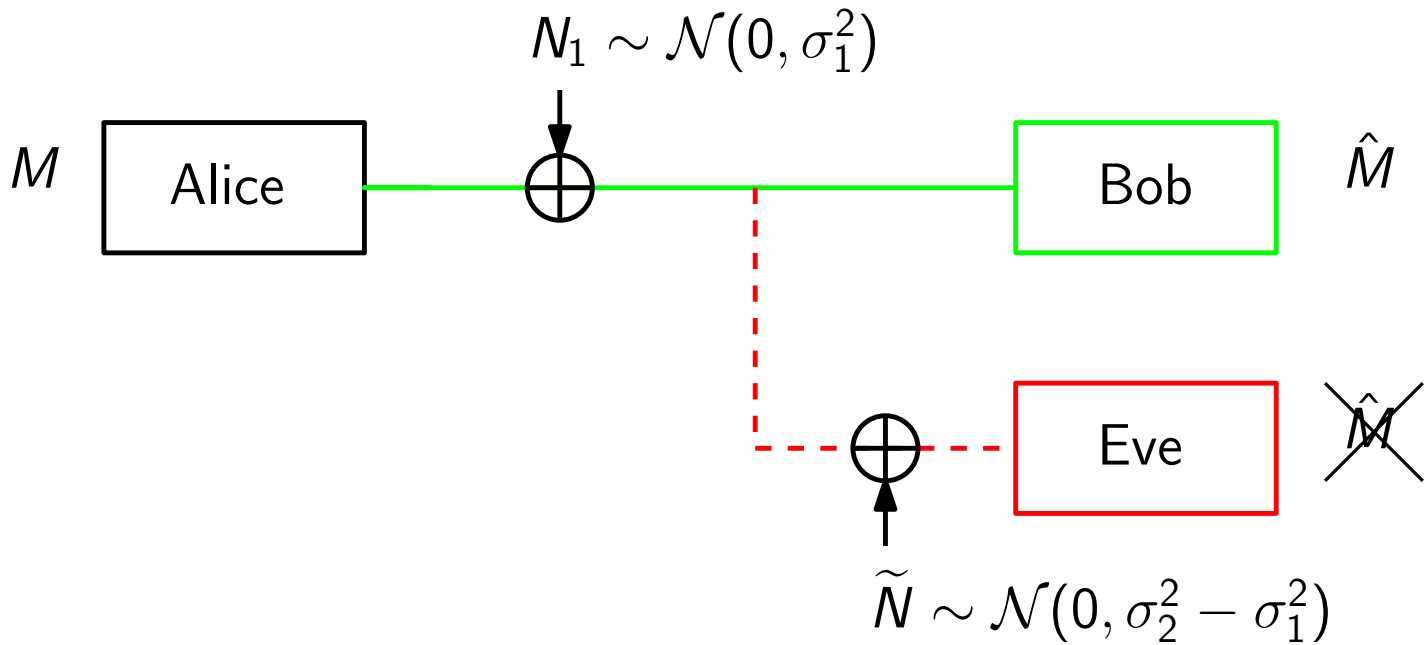
The Gaussian wiretap channel (contd.)

- Secrecy capacity depends on $p(x, y)$ and $p(x, z)$, **not** $p(x, y, z)$.



The Gaussian wiretap channel (contd.)

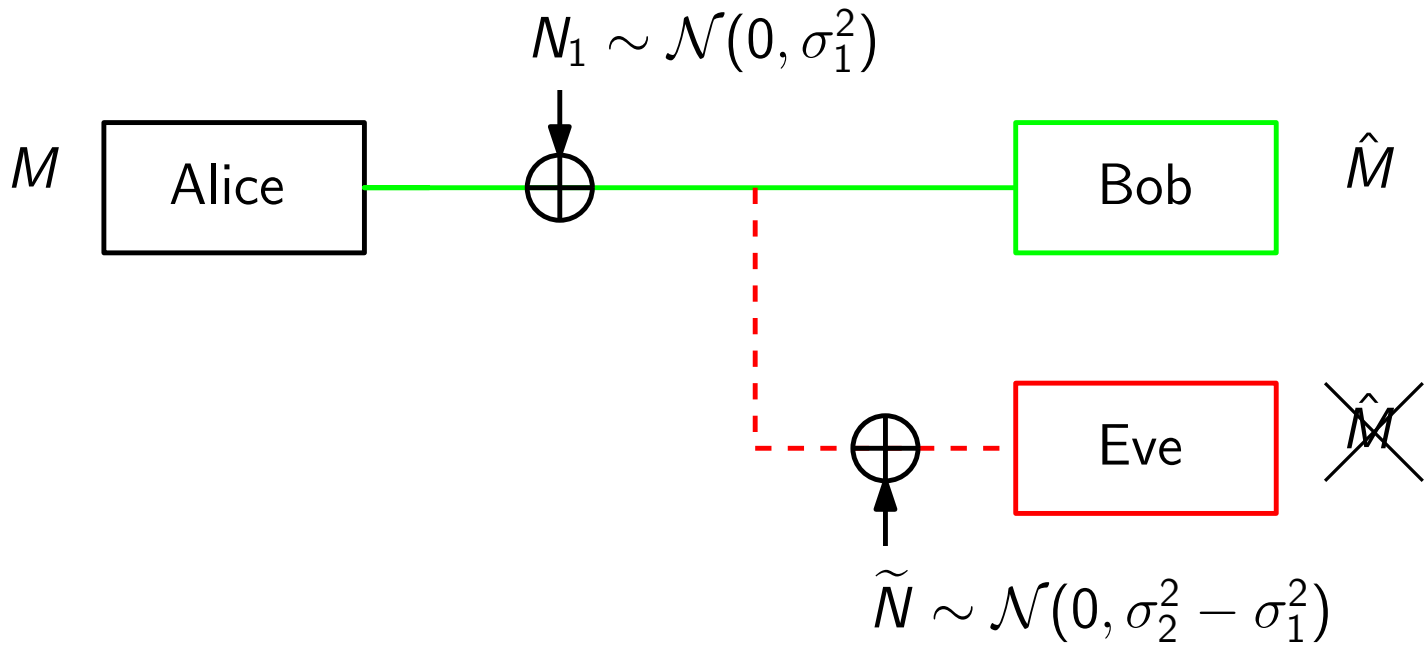
- Secrecy capacity depends on $p(x, y)$ and $p(x, z)$, **not** $p(x, y, z)$.



- The degraded version has same secrecy capacity.

The Gaussian wiretap channel (contd.)

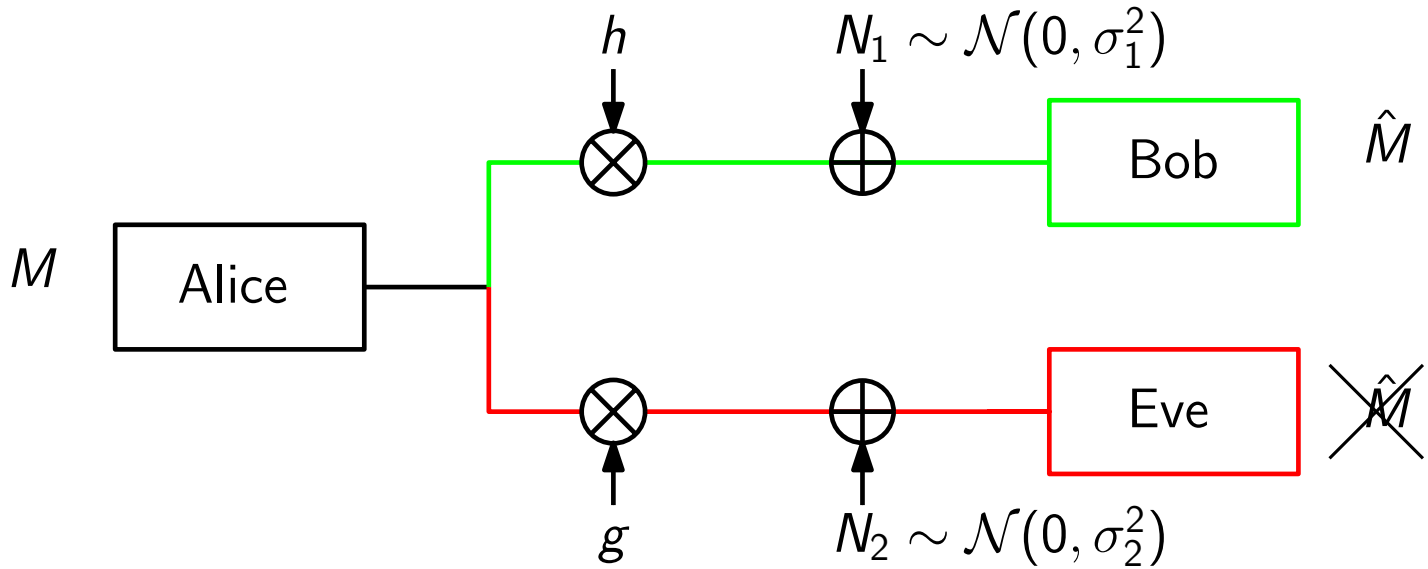
- Secrecy capacity depends on $p(x, y)$ and $p(x, z)$, **not** $p(x, y, z)$.



- The degraded version has same secrecy capacity.
- Apply Wyner's result on the degraded wiretap channel.

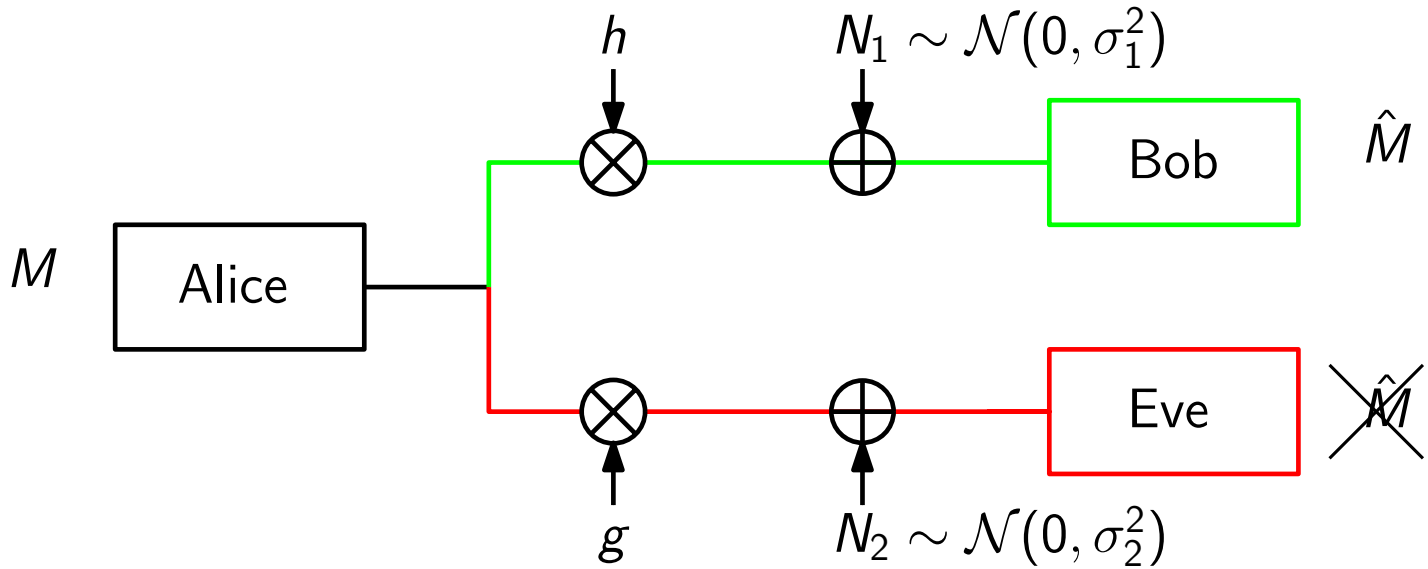
The wireless fading wiretap channel

- A wireless scenario with Rayleigh fading.



The wireless fading wiretap channel

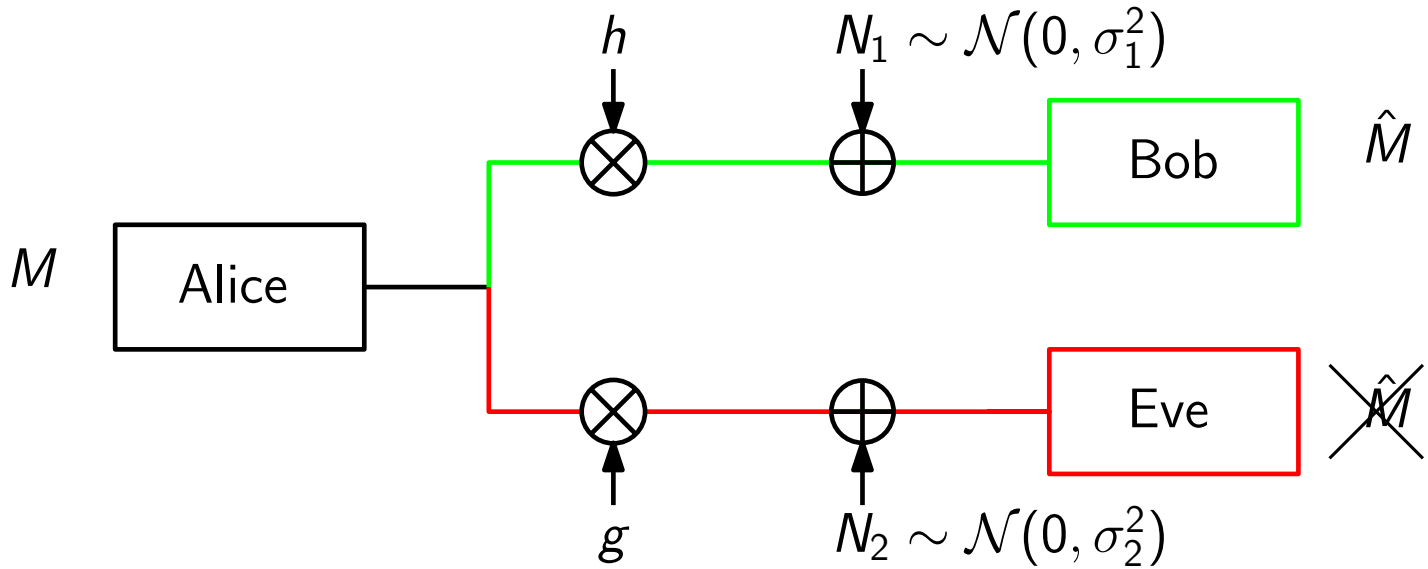
- A wireless scenario with Rayleigh fading.



- h, g correspond to Rayleigh fading model.

The wireless fading wiretap channel

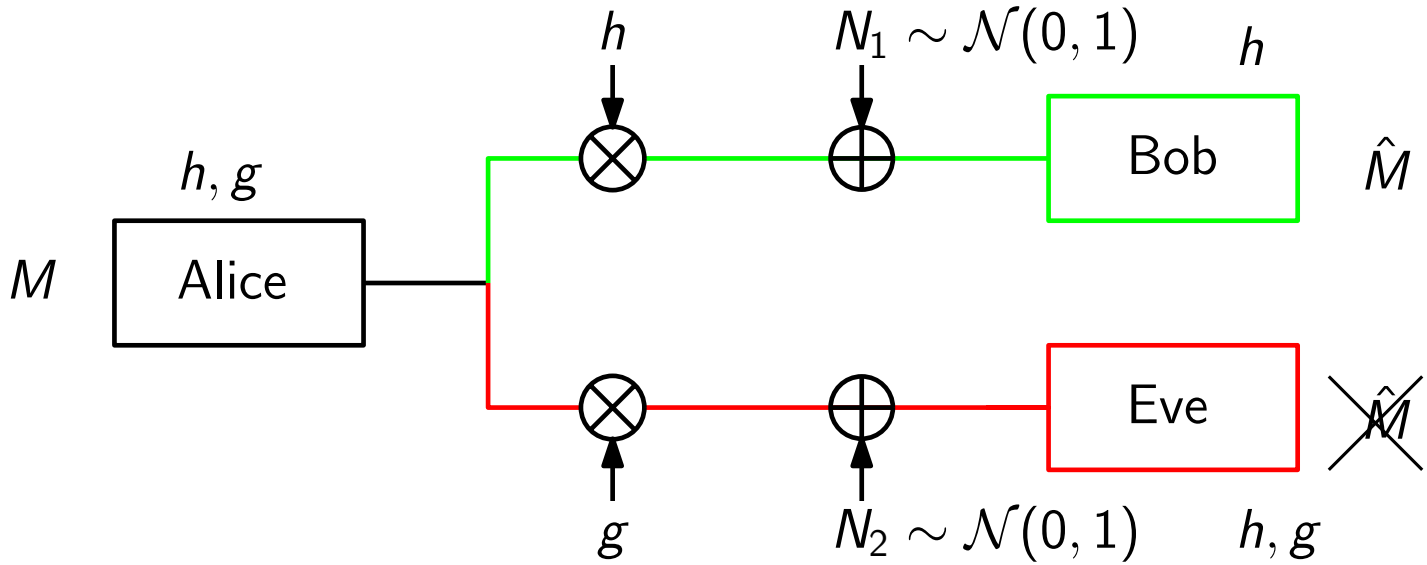
- A wireless scenario with Rayleigh fading.



- h, g correspond to Rayleigh fading model.
- Secrecy capacity will depend on availablility of CSI.

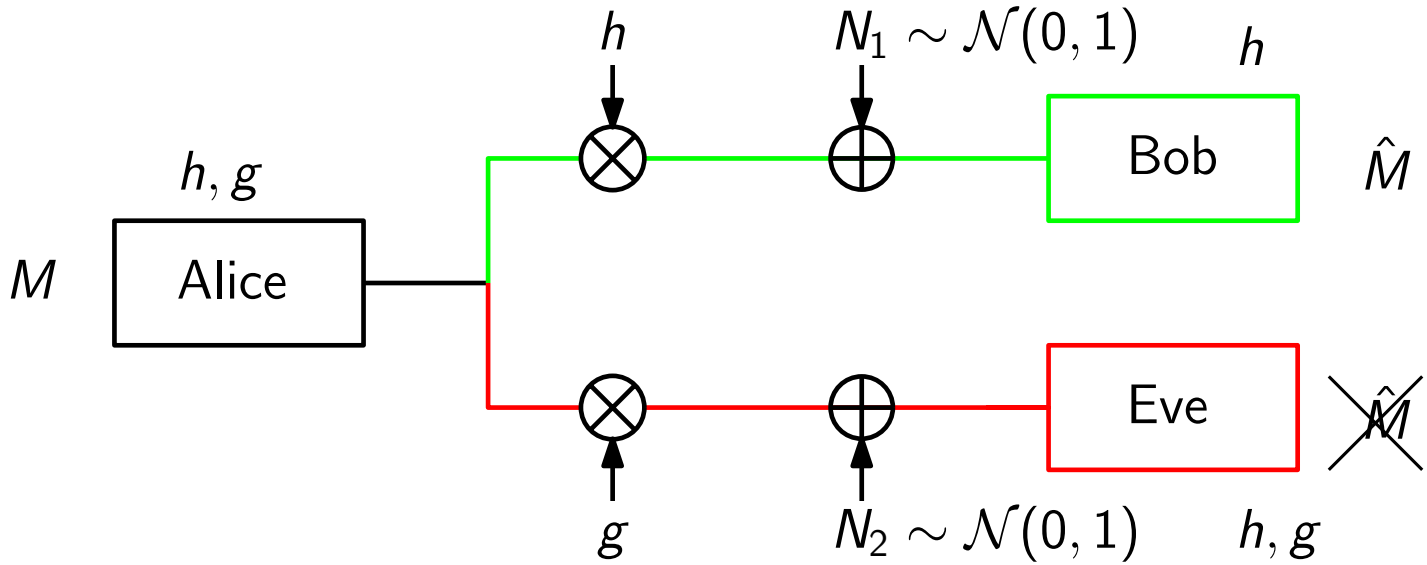
Fading wiretap channel with full CSIT, CSIR

- Liang-Poor-Shamai, Li-Yates-Trappe,Gopala-Lai-El Gamal.



Fading wiretap channel with full CSIT, CSIR

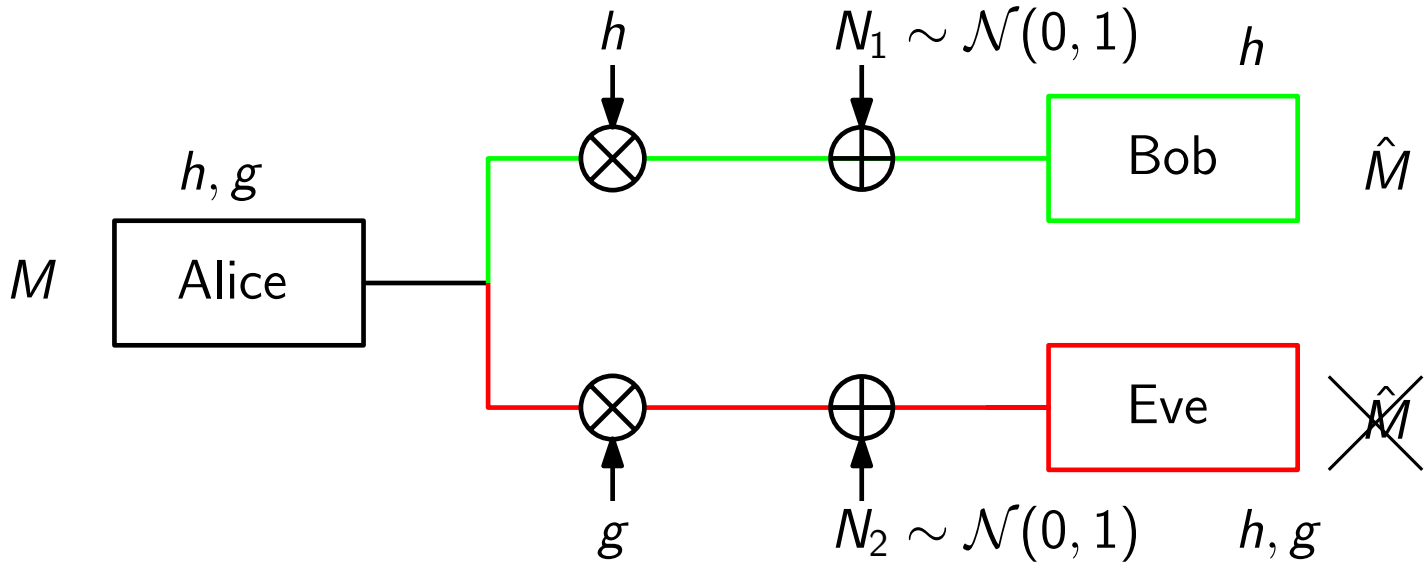
- Liang-Poor-Shamai, Li-Yates-Trappe,Gopala-Lai-El Gamal.



- Equivalent to independent parallel channels.

Fading wiretap channel with full CSIT, CSIR

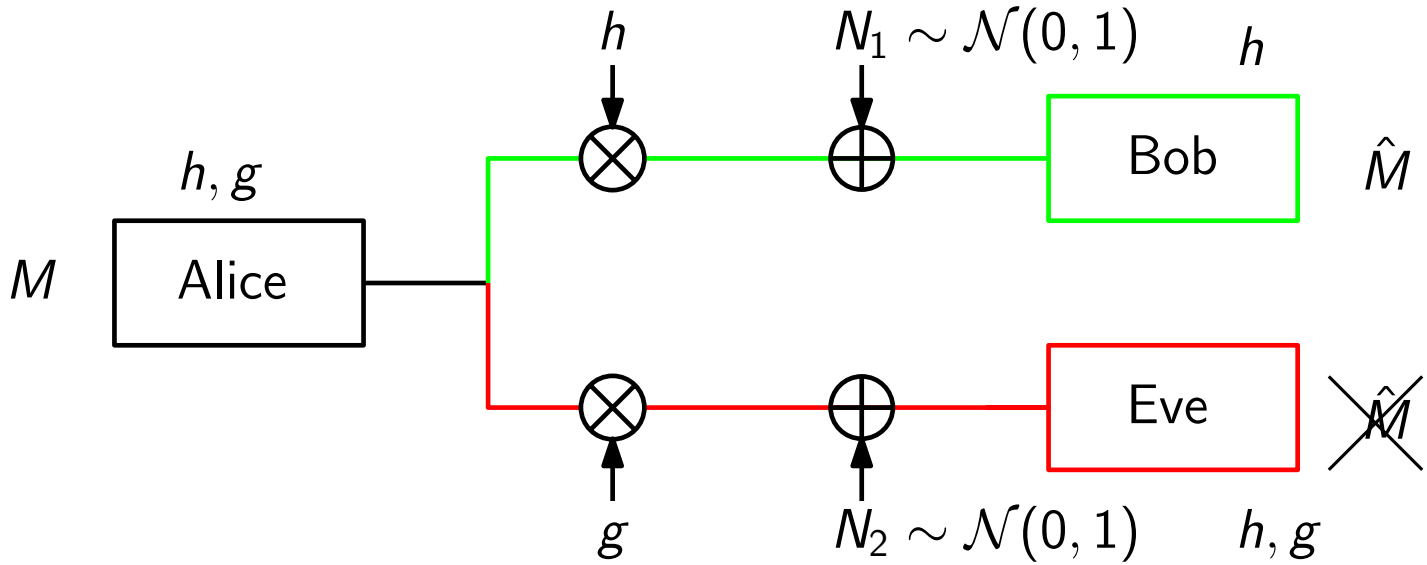
- Liang-Poor-Shamai, Li-Yates-Trappe,Gopala-Lai-El Gamal.



- Equivalent to independent parallel channels.
- Independent Gaussian signaling is optimal.

Fading wiretap channel with full CSIT, CSIR

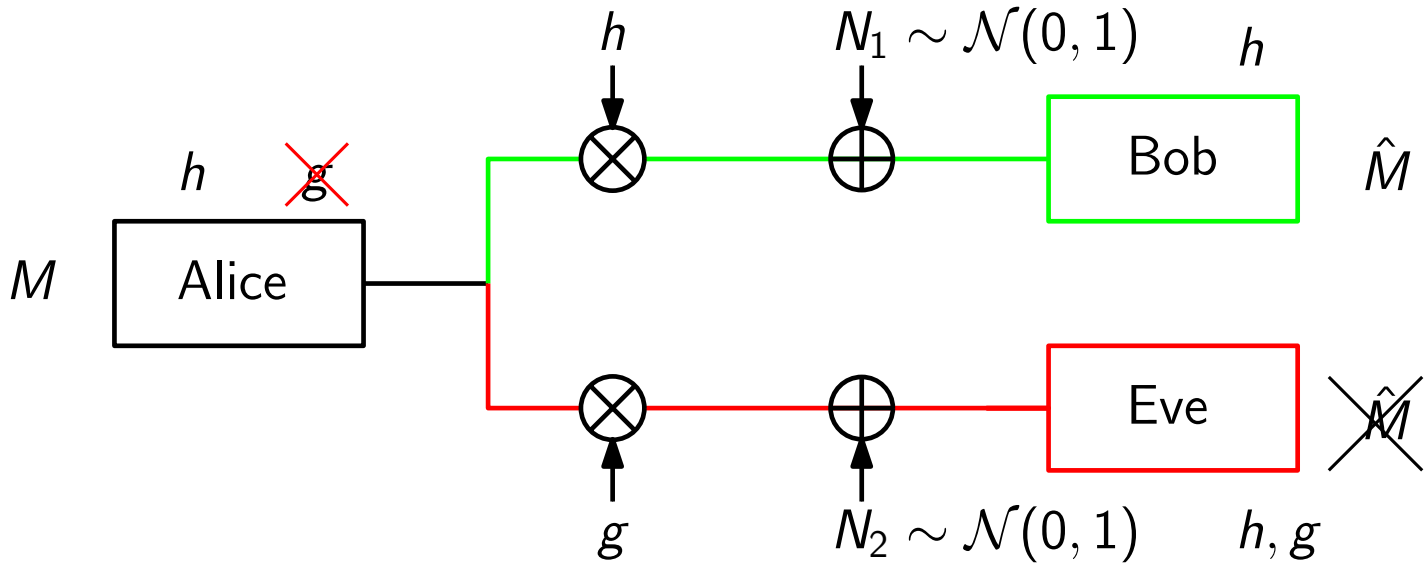
- Liang-Poor-Shamai, Li-Yates-Trappe,Gopala-Lai-El Gamal.



- Equivalent to independent parallel channels.
- Independent Gaussian signaling is optimal.
- Power allocation using water-filling.

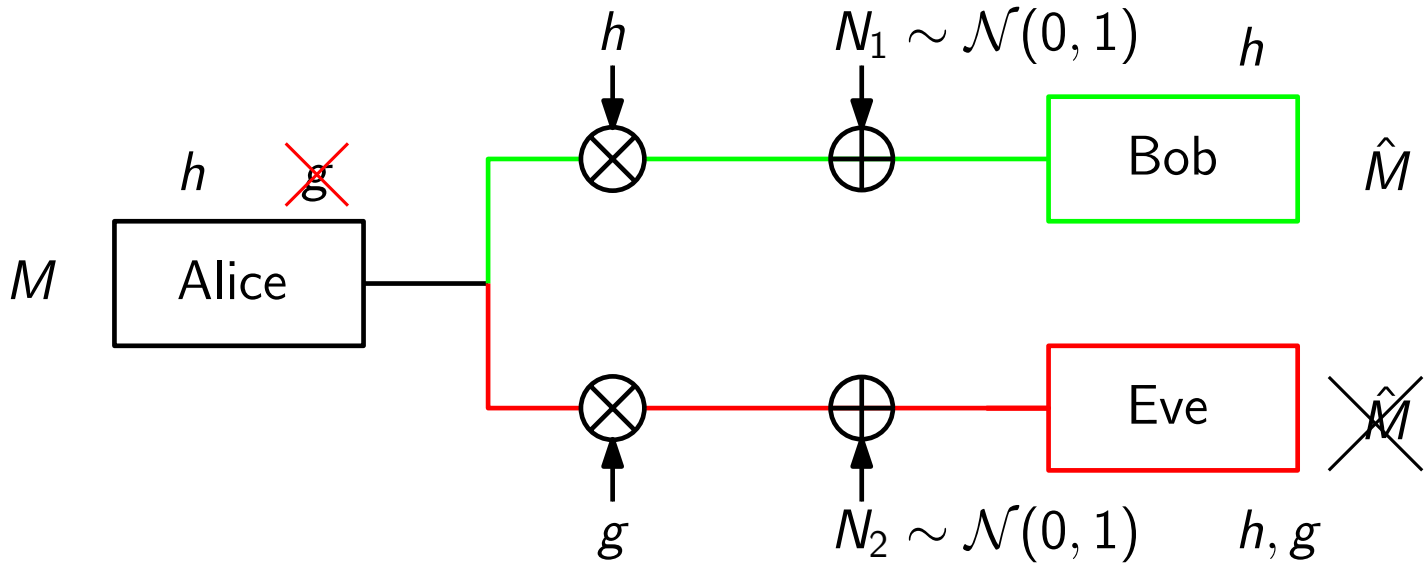
Fading wiretap channel with main channel CSIT

- Gopala, Lai, El Gamal, 2008.



Fading wiretap channel with main channel CSIT

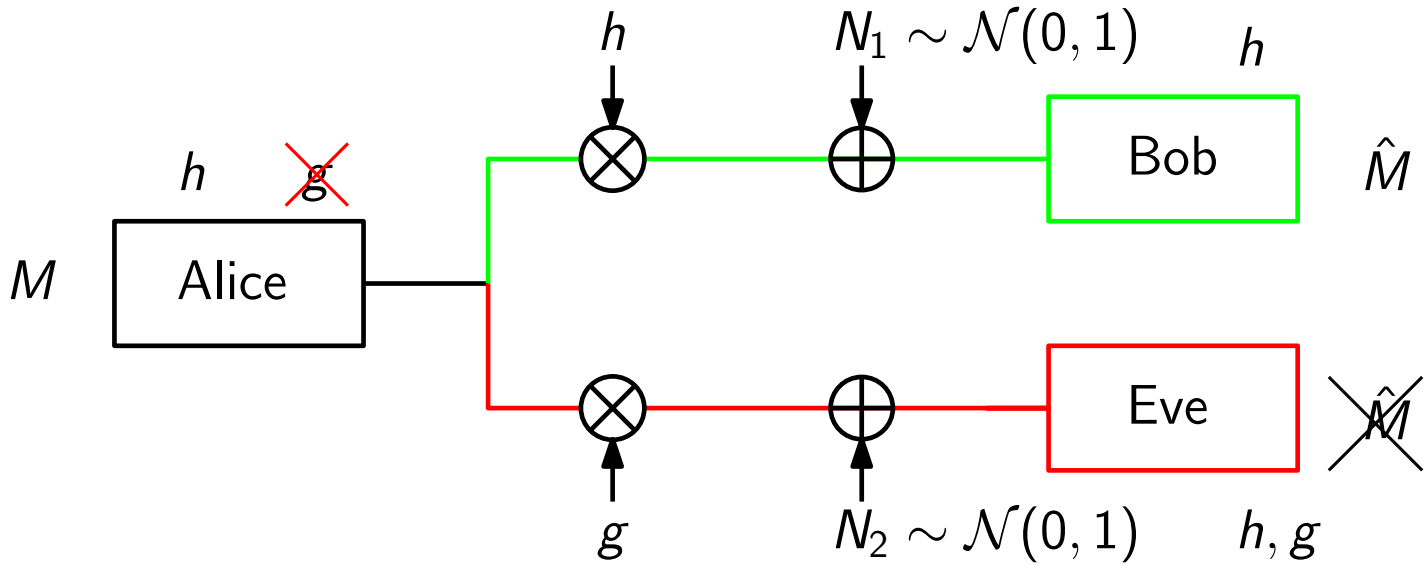
- Gopala, Lai, El Gamal, 2008.



- Codelength $\gg$ Coherence time $\gg 1$

Fading wiretap channel with main channel CSIT

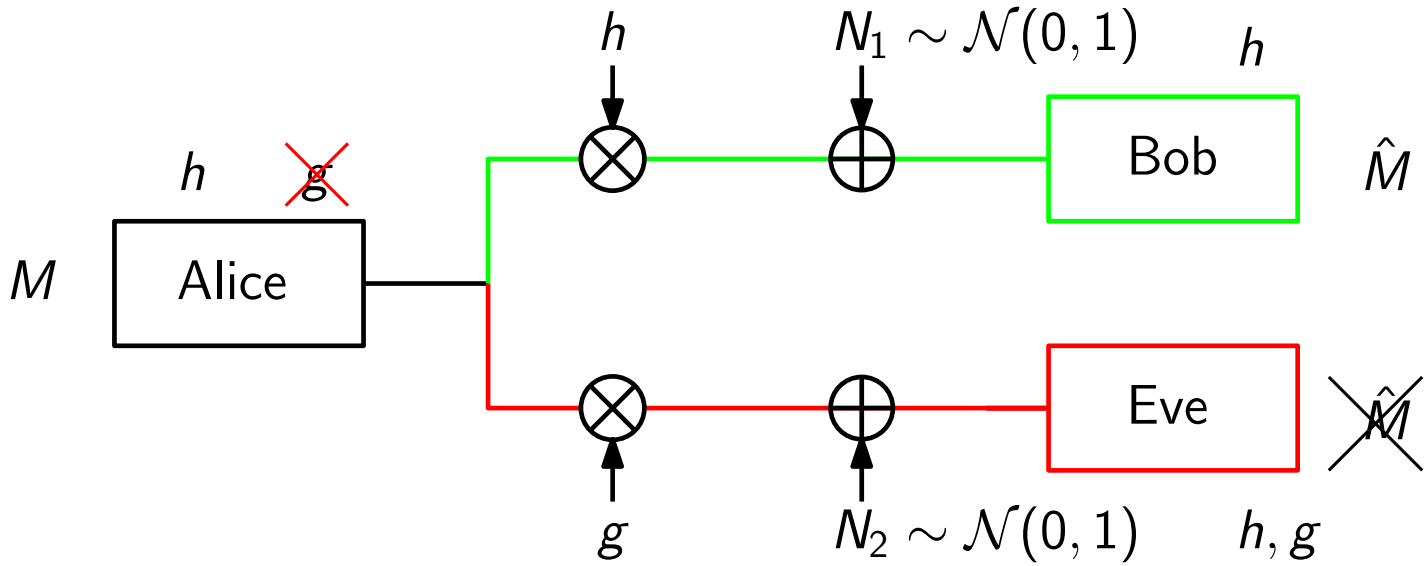
- Gopala, Lai, El Gamal, 2008.



- Codelength $\gg$ Coherence time $\gg 1$
- **Only** main channel CSI available at Alice.

Fading wiretap channel with main channel CSIT

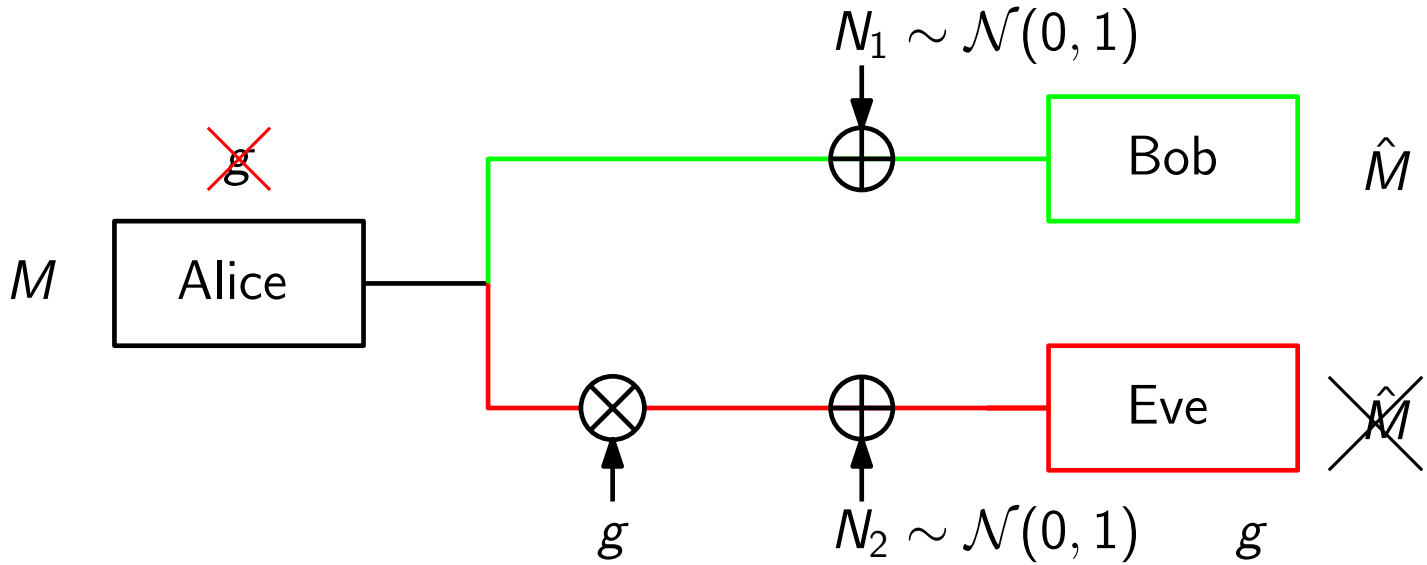
- Gopala, Lai, El Gamal, 2008.



- Codelength $\gg$ Coherence time $\gg 1$
- **Only** main channel CSI available at Alice.
- **Variable-rate** transmission scheme with Gaussian signaling is optimal.

Fading wiretap channel with main channel CSIT

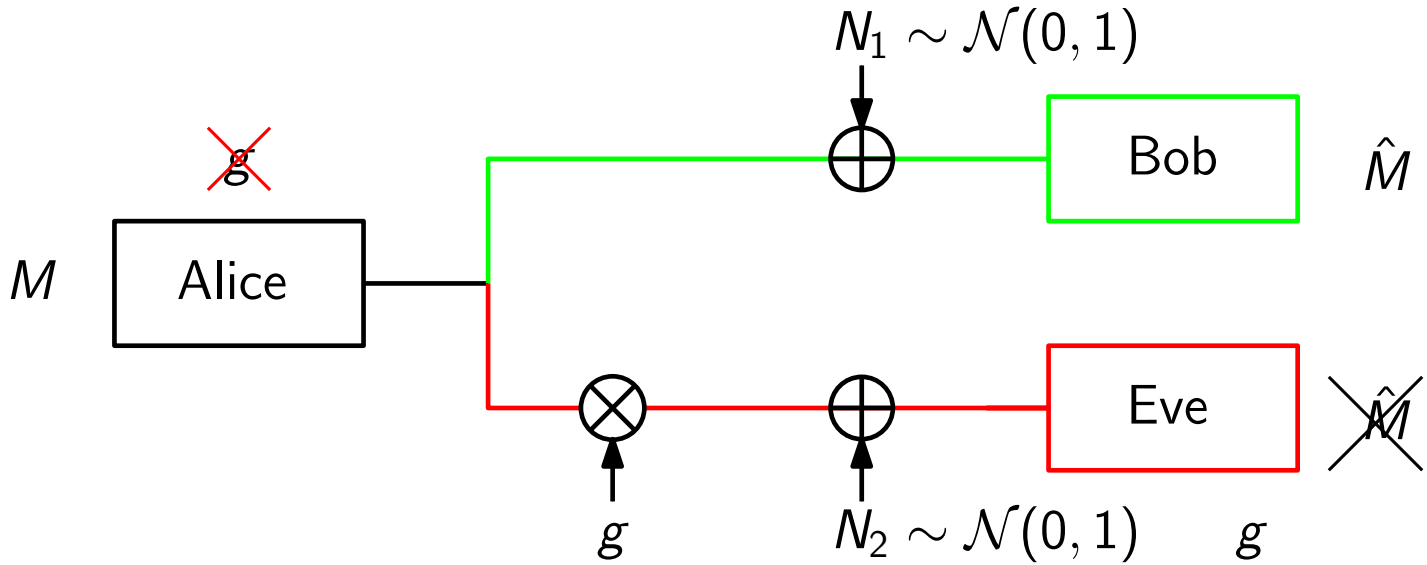
- Li, Yates, Trappe, 2010.



- **Fixed** main channel, **fading** eavesdropper channel.

Fading wiretap channel with main channel CSIT

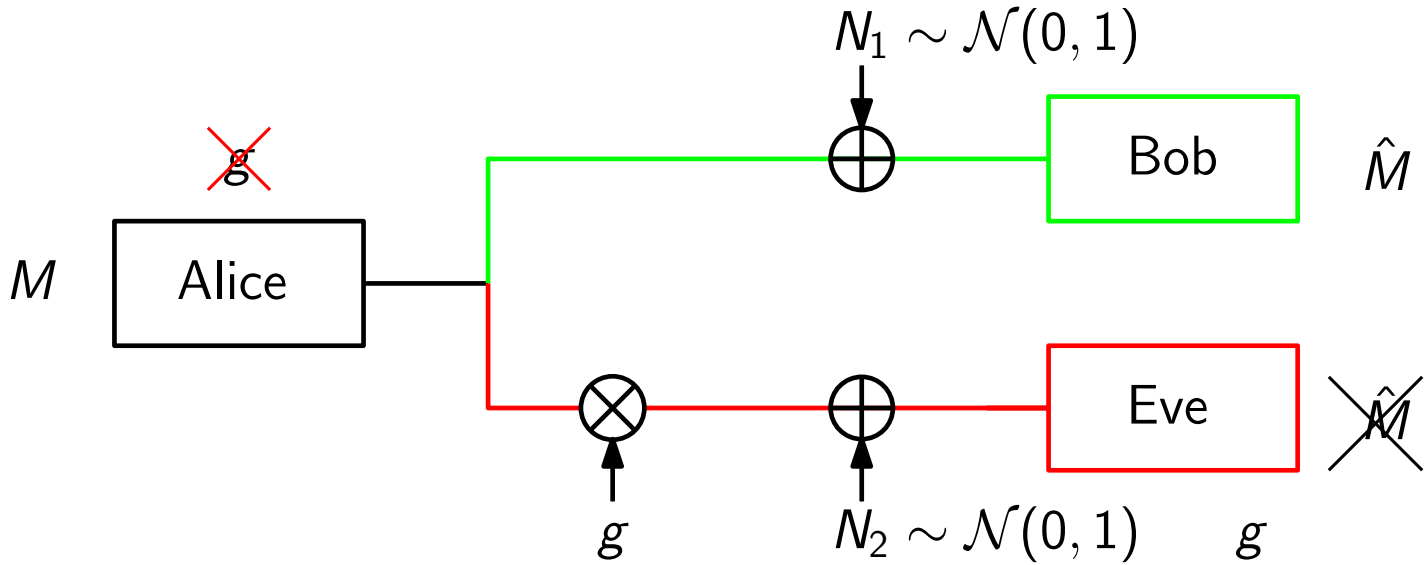
- Li, Yates, Trappe, 2010.



- **Fixed** main channel, **fading** eavesdropper channel.
- Codelength $\gg$ Coherence time $= 1$

Fading wiretap channel with main channel CSIT

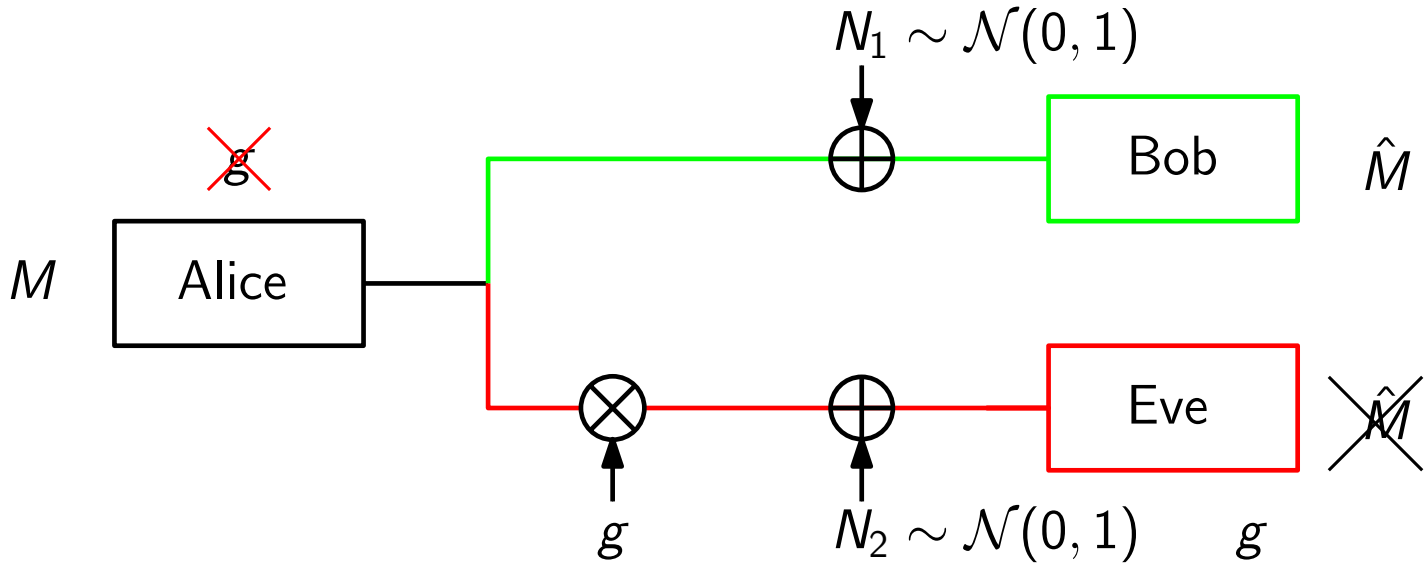
- Li, Yates, Trappe, 2010.



- **Fixed** main channel, **fading** eavesdropper channel.
- Codelength $\gg$ Coherence time $= 1$
- When main channel is better, Gaussian signaling is almost optimal.

Fading wiretap channel with main channel CSIT

- Li, Yates, Trappe, 2010.



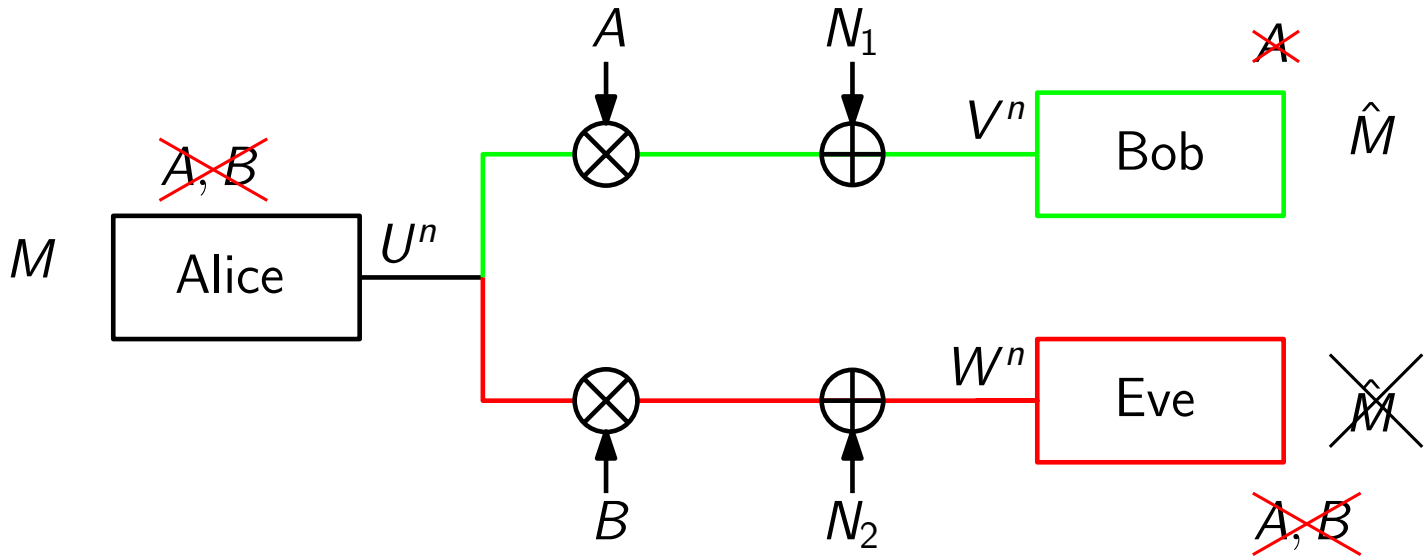
- **Fixed** main channel, **fading** eavesdropper channel.
- Codelength $\gg$ Coherence time $= 1$
- When main channel is better, Gaussian signaling is almost optimal.
- When main channel is worse, M-QAM outperforms Gaussian signaling with artificial noise and bursting.

Fading wiretap channel with no CSI anywhere

- *Very* fast fading scenario: small coherence time.

Fading wiretap channel with no CSI anywhere

- *Very* fast fading scenario: small coherence time.
- Training requires too much overhead.

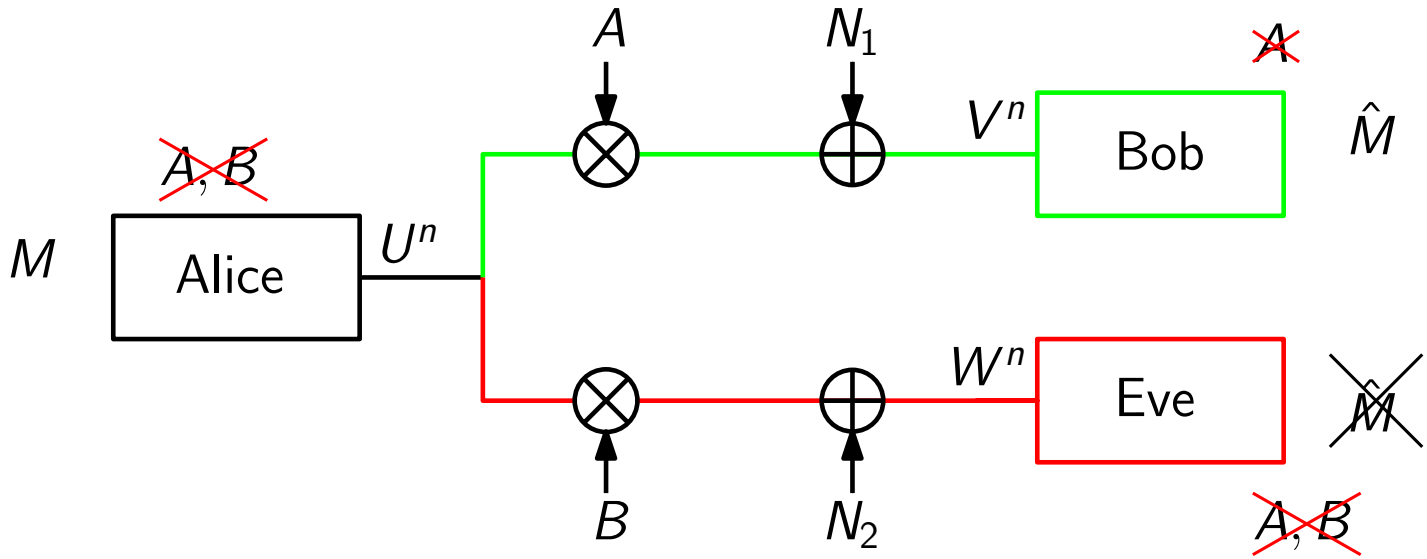


$$N_1 \sim \mathcal{CN}(0, \frac{1}{2}\sigma_1^2 I) \qquad N_2 \sim \mathcal{CN}(0, \frac{1}{2}\sigma_2^2 I)$$

$$V = AU + N_1$$
$$W = BU + N_2$$

Fading wiretap channel with no CSI anywhere

- *Very* fast fading scenario: small coherence time.
- Training requires too much overhead.



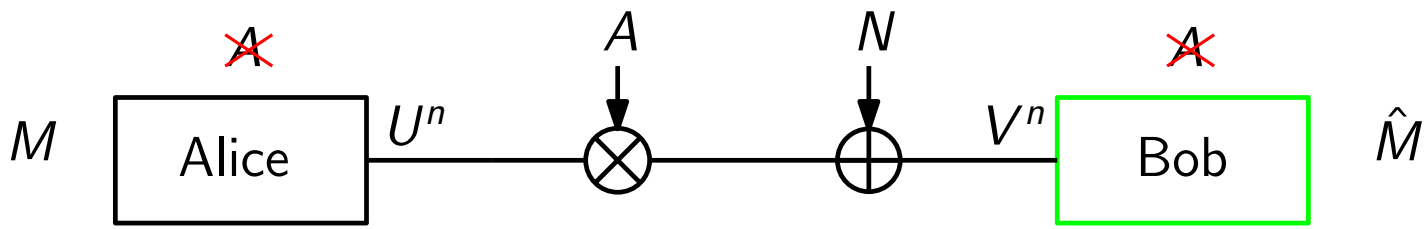
$$N_1 \sim \mathcal{CN}(0, \frac{1}{2}\sigma_1^2 I) \qquad N_2 \sim \mathcal{CN}(0, \frac{1}{2}\sigma_2^2 I)$$

$$V = AU + N_1$$
$$W = BU + N_2$$

- Wiretap extension of Abou-Faycal, Trott, Shamai (2001).

Fading channel with no CSI anywhere

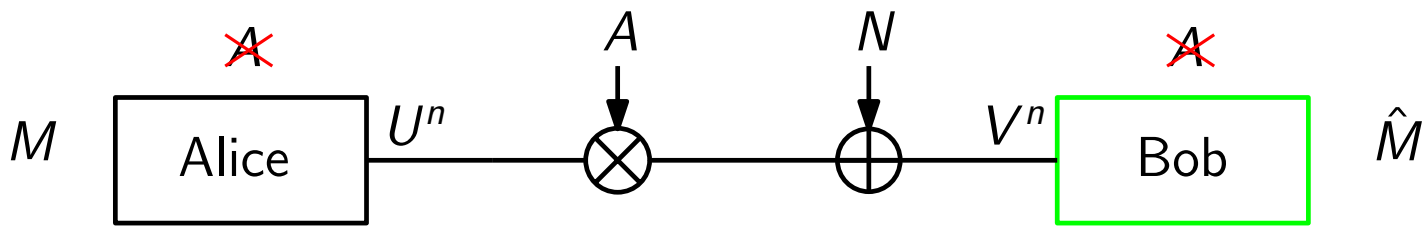
- Studied by Abou-Faycal, Trott, Shamai (2001).



$$V = AU + N$$

Fading channel with no CSI anywhere

- Studied by Abou-Faycal, Trott, Shamai (2001).

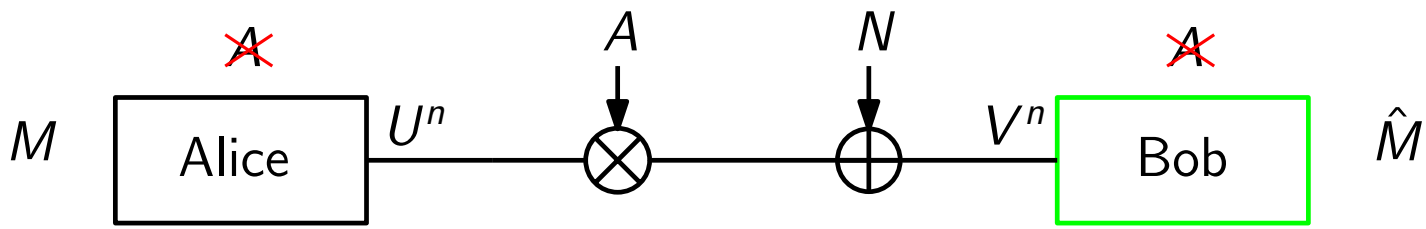


$$V = AU + N$$

- Rayleigh fast fading with coherence time 1.

Fading channel with no CSI anywhere

- Studied by Abou-Faycal, Trott, Shamai (2001).

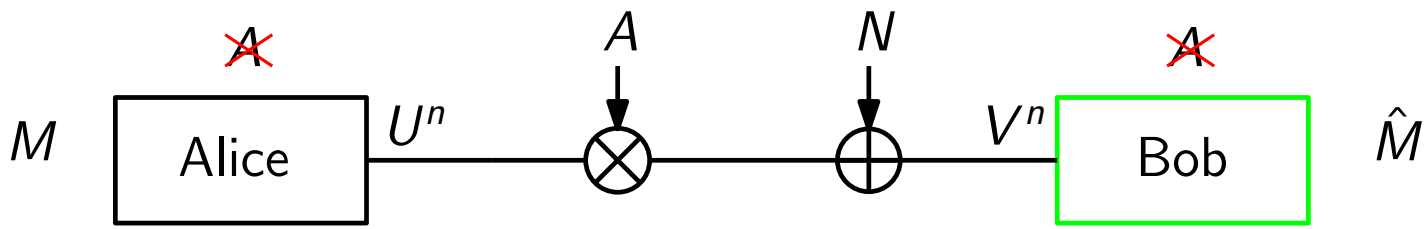


$$V = AU + N$$

- Rayleigh fast fading with coherence time 1.
- The channel fading coefficients A is not known to any user.

Fading channel with no CSI anywhere

- Studied by Abou-Faycal, Trott, Shamai (2001).

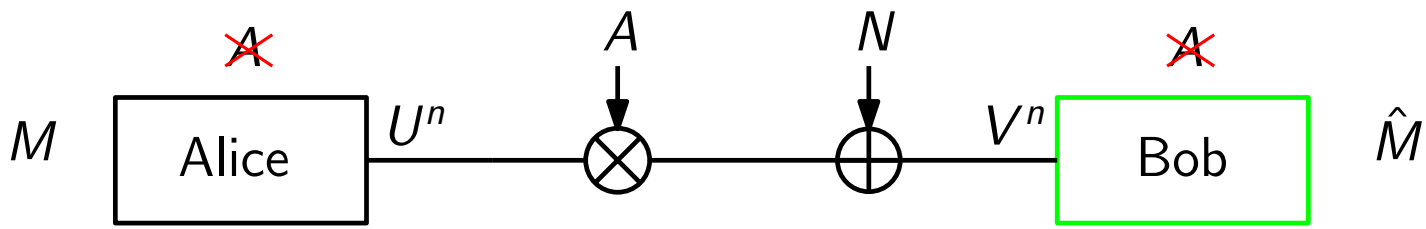


$$V = AU + N$$

- Rayleigh fast fading with coherence time 1.
- The channel fading coefficients A is not known to any user.
- The phase does not carry any information.

Fading channel with no CSI anywhere

- Studied by Abou-Faycal, Trott, Shamai (2001).

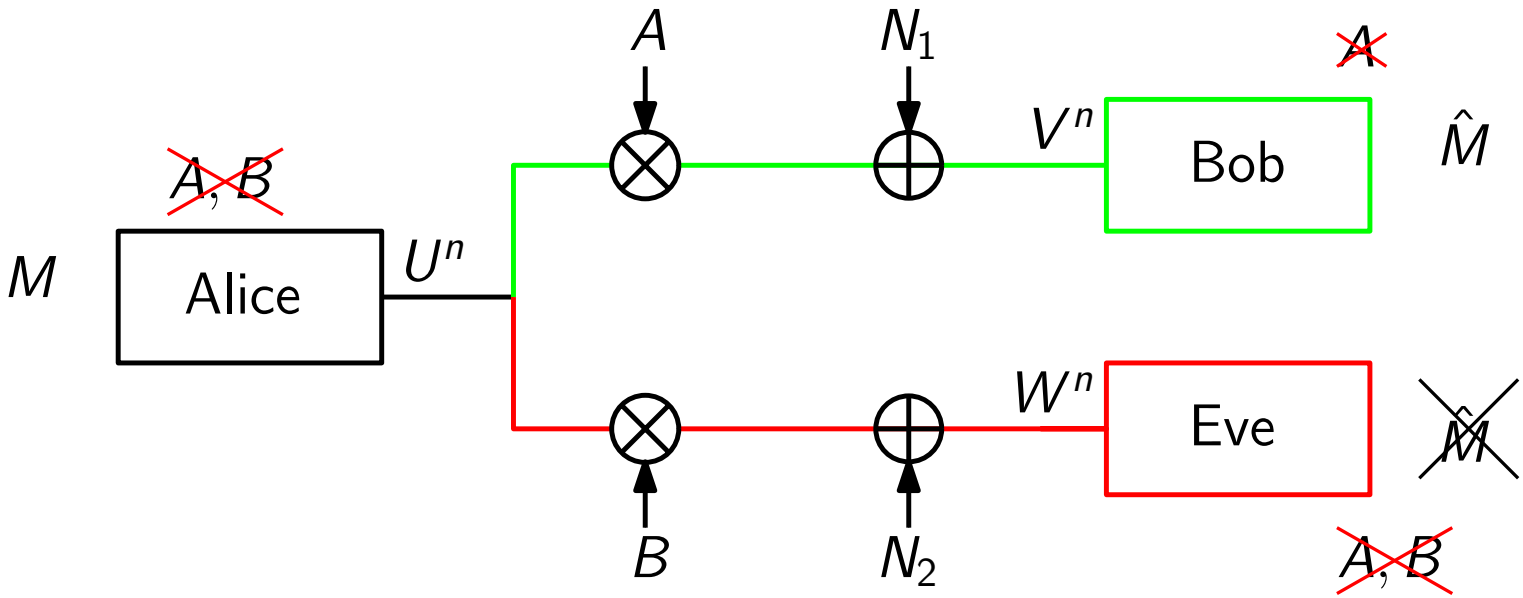


$$V = AU + N$$

- Rayleigh fast fading with coherence time 1.
- The channel fading coefficients A is not known to any user.
- The phase does not carry any information.
- The optimal input distribution is discrete with a finite number of mass points.

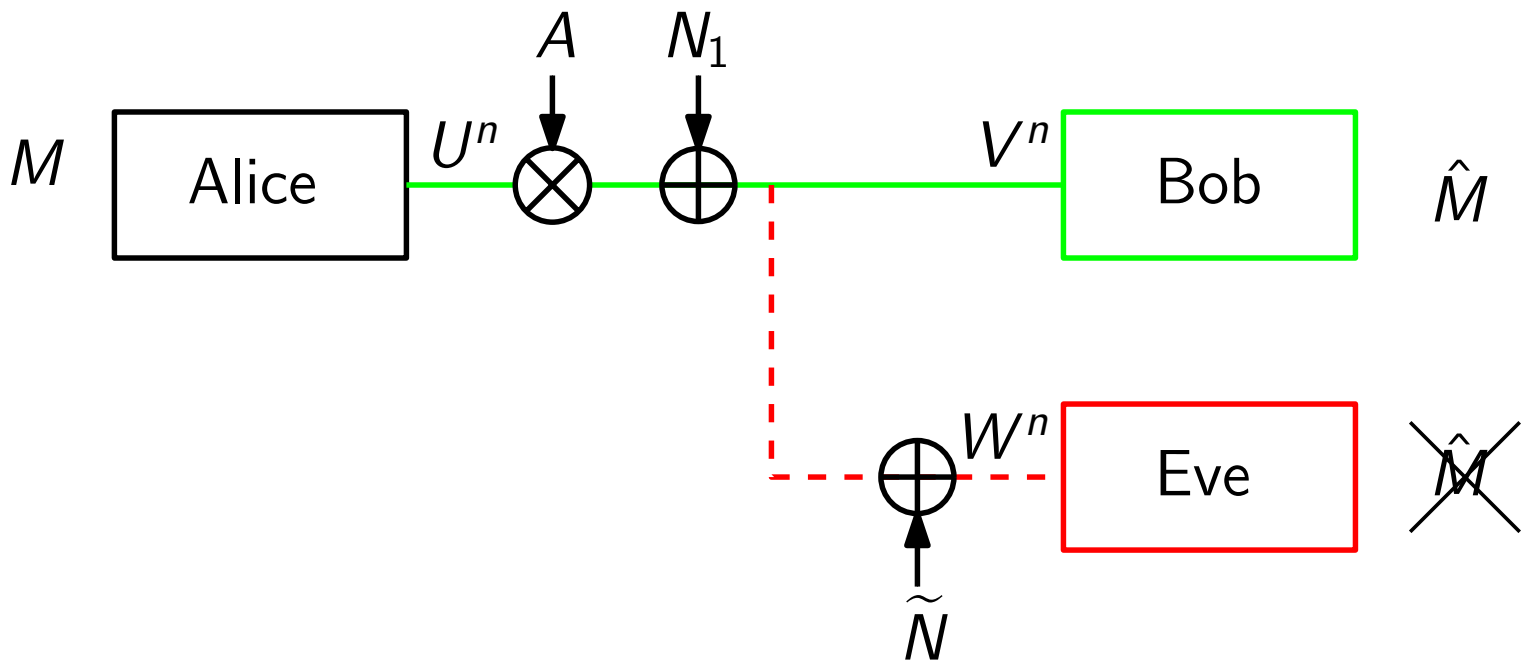
Equivalent degraded wiretap channel

- The secrecy capacity depends only on the marginal distributions $p(u, v)$ and $p(u, w)$, **not** $p(u, v, w)$.



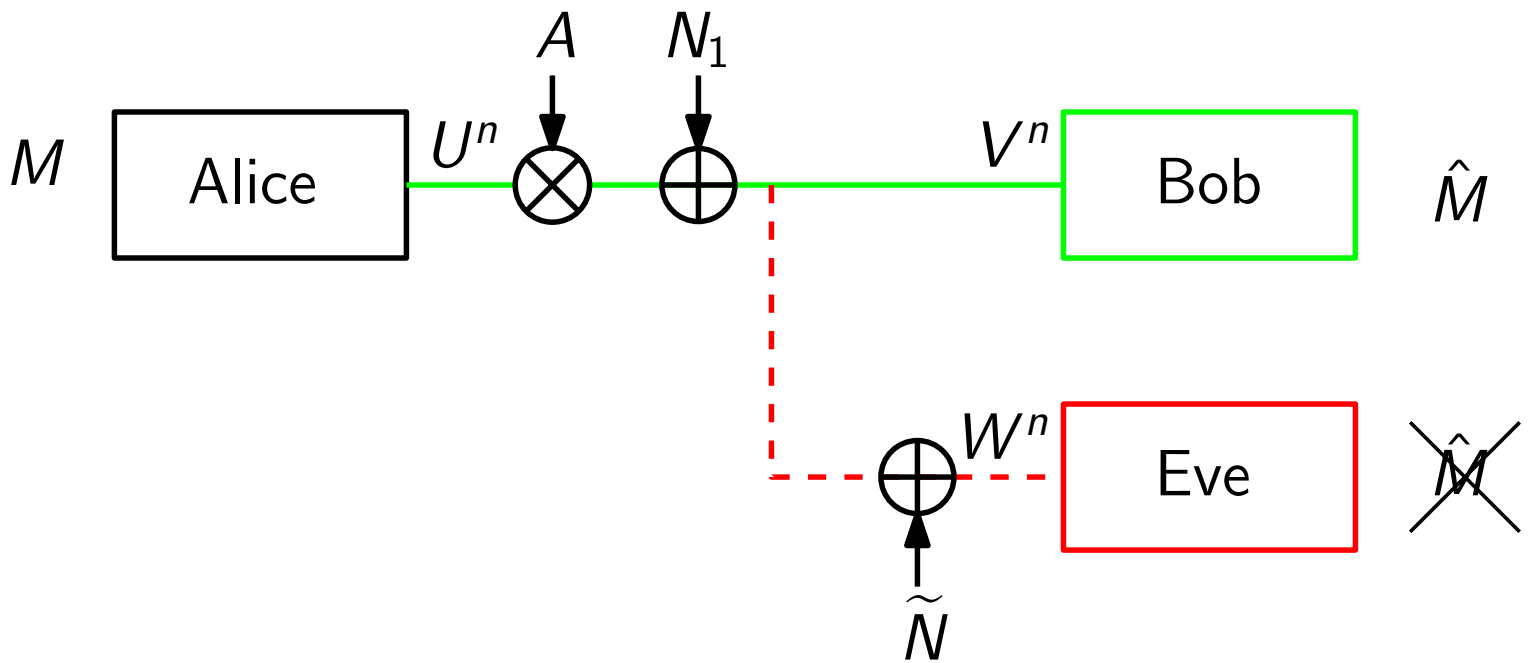
Equivalent degraded wiretap channel

- The secrecy capacity depends only on the marginal distributions $p(u, v)$ and $p(u, w)$, **not** $p(u, v, w)$.



Equivalent degraded wiretap channel

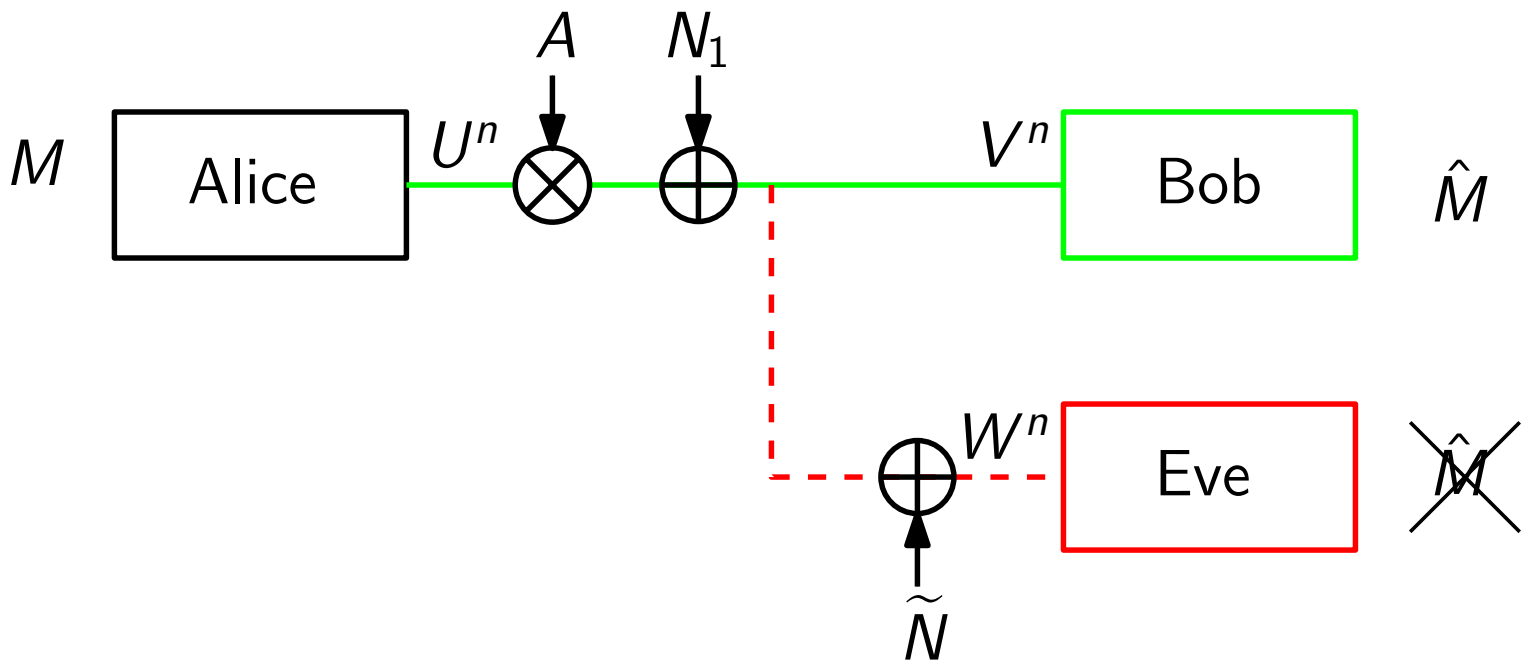
- The secrecy capacity depends only on the marginal distributions $p(u, v)$ and $p(u, w)$, **not** $p(u, v, w)$.



- Equivalent with respect to secrecy capacity.

Equivalent degraded wiretap channel

- The secrecy capacity depends only on the marginal distributions $p(u, v)$ and $p(u, w)$, **not** $p(u, v, w)$.



  - Equivalent with respect to secrecy capacity.
  - Apply Wyner's result.

The optimization problem

- Wyner's result yields

$$C_s = \sup_{F \in \mathcal{F}} I(U;V) - I(U;W)$$

where F : distribution of U and $\mathcal{F} = \left\{ F : \mathbb{E}_F \left[|U|^2 \right] \leq P \right\}$

The optimization problem

- Wyner's result yields

$$C_s = \sup_{F \in \mathcal{F}} I(U;V) - I(U;W)$$

where F : distribution of U and $\mathcal{F} = \left\{F : \mathbb{E}_F\left[|U|^2\right] \leq P\right\}$

- Phase carries **no** information, so, if $X = |U|$, $Y = |V|^2$, $Z = |W|^2$,

$$I(U;V) = I(X;Y) \text{ and } I(U;W) = I(X;Z)$$

The optimization problem

- Wyner's result yields

$$C_s = \sup_{F \in \mathcal{F}} I(U;V) - I(U;W)$$

where F : distribution of U and $\mathcal{F} = \left\{F : \mathbb{E}_F\left[|U|^2\right] \leq P\right\}$

- Phase carries **no** information, so, if $X = |U|$, $Y = |V|^2$, $Z = |W|^2$,

$$I(U;V) = I(X;Y) \text{ and } I(U;W) = I(X;Z)$$

- Simplified secrecy capacity expression:

$$C_s = \sup_{F \in \mathcal{F}} I(X;Y) - I(X;Z)$$

The optimization problem

- Wyner's result yields

$$C_s = \sup_{F \in \mathcal{F}} I(U;V) - I(U;W)$$

  where F : distribution of U and $\mathcal{F} = \left\{F : \mathbb{E}_F\left[|U|^2\right] \leq P\right\}$
- Phase carries **no** information, so, if $X = |U|$, $Y = |V|^2$, $Z = |W|^2$,

$$I(U;V) = I(X;Y) \text{ and } I(U;W) = I(X;Z)$$

- Simplified secrecy capacity expression:

$$C_s = \sup_{F \in \mathcal{F}} I(X;Y) - I(X;Z)$$

- Prove $X \to Y \to Z$.

The optimization problem

- Wyner's result yields

$$C_s = \sup_{F \in \mathcal{F}} I(U;V) - I(U;W)$$

  where F : distribution of U and $\mathcal{F} = \left\{F : \mathbb{E}_F\left[|U|^2\right] \leq P\right\}$
- Phase carries **no** information, so, if $X = |U|$, $Y = |V|^2$, $Z = |W|^2$,

$$I(U;V) = I(X;Y) \text{ and } I(U;W) = I(X;Z)$$

- Simplified secrecy capacity expression:

$$C_s = \sup_{F \in \mathcal{F}} I(X;Y) - I(X;Z)$$

- Prove $X \to Y \to Z$.
- Generalize van Dijk: convex optimization problem.

The optimization problem (contd.)

- Functional optimization problem: Smith (1971).

The optimization problem (contd.)

- Functional optimization problem: Smith (1971).
- Abou-Faycal, Trott, Shamai: the supremum is achieved.

The optimization problem (contd.)

- Functional optimization problem: Smith (1971).
- Abou-Faycal, Trott, Shamai: the supremum is achieved.
- With Langrange multipliers, KKT optimality conditions:

$$f(x) = \gamma(x^2 - P) + C_s - i(x;y) + i(x;z) \geq 0, \ \forall x \in \mathbb{R}$$

with equality iff $x \in \operatorname{supp} X^*$, and,

$$i(x;y) = \int p(y|x) \log \frac{p(y|x)}{p(y)} \, dy$$

$$\text{with} \ \ p(y) = \int p(y|x) dF_X^*$$

The optimization problem (contd.)

- Functional optimization problem: Smith (1971).
- Abou-Faycal, Trott, Shamai: the supremum is achieved.
- With Langrange multipliers, KKT optimality conditions:

$$f(x) = \gamma(x^2 - P) + C_s - i(x;y) + i(x;z) \geq 0, \ \forall x \in \mathbb{R}$$

with equality iff $x \in \operatorname{supp} X^*$, and,

$$i(x;y) = \int p(y|x) \log \frac{p(y|x)}{p(y)} \, dy$$

$$\text{with} \ \ p(y) = \int p(y|x) dF_X^*$$

- Analyse KKT conditions to get the results.

Results

Theorem 1: The optimal X^* is **discrete** with at most finite number of points in any bounded interval.

Results

Theorem 1: The optimal X^* is **discrete** with at most finite number of points in any bounded interval.

Outline of proof:

Results

Theorem 1: The optimal X^* is **discrete** with at most finite number of points in any bounded interval.

Outline of proof:

- Proof by contradiction.

Results

Theorem 1: The optimal X^* is **discrete** with at most finite number of points in any bounded interval.

Outline of proof:

- Proof by contradiction.
- Recall the KKT conditions:

$$\begin{aligned} f(x) \geq & 0, \quad \forall x \in \mathbb{R} \\ f(x) = & 0, \quad x \in E = \operatorname{supp} X^* \end{aligned}$$

Results

Theorem 1: The optimal X^* is **discrete** with at most finite number of points in any bounded interval.

Outline of proof:

- Proof by contradiction.
- Recall the KKT conditions:

$$\begin{aligned} f(x) \geq & 0, \quad \forall x \in \mathbb{R} \\ f(x) = & 0, \quad x \in E = \operatorname{supp} X^* \end{aligned}$$

- Assume E contains infinitely many points with a converging subsequence.

Results

Theorem 1: The optimal X^* is **discrete** with at most finite number of points in any bounded interval.

Outline of proof:

- Proof by contradiction.
- Recall the KKT conditions:

$$\begin{aligned} f(x) \geq & 0, \quad \forall x \in \mathbb{R} \\ f(x) = & 0, \quad x \in E = \operatorname{supp} X^* \end{aligned}$$

- Assume E contains infinitely many points with a converging subsequence.
- Observe that f extends analytically to the complex plane.

Results

Theorem 1: The optimal X^* is **discrete** with at most finite number of points in any bounded interval.

Outline of proof:

- Proof by contradiction.
- Recall the KKT conditions:

$$\begin{aligned} f(x) \geq & 0, \quad \forall x \in \mathbb{R} \\ f(x) = & 0, \quad x \in E = \operatorname{supp} X^* \end{aligned}$$

- Assume E contains infinitely many points with a converging subsequence.
- Observe that f extends analytically to the complex plane.
- Using the *Identity theorem*, conclude that

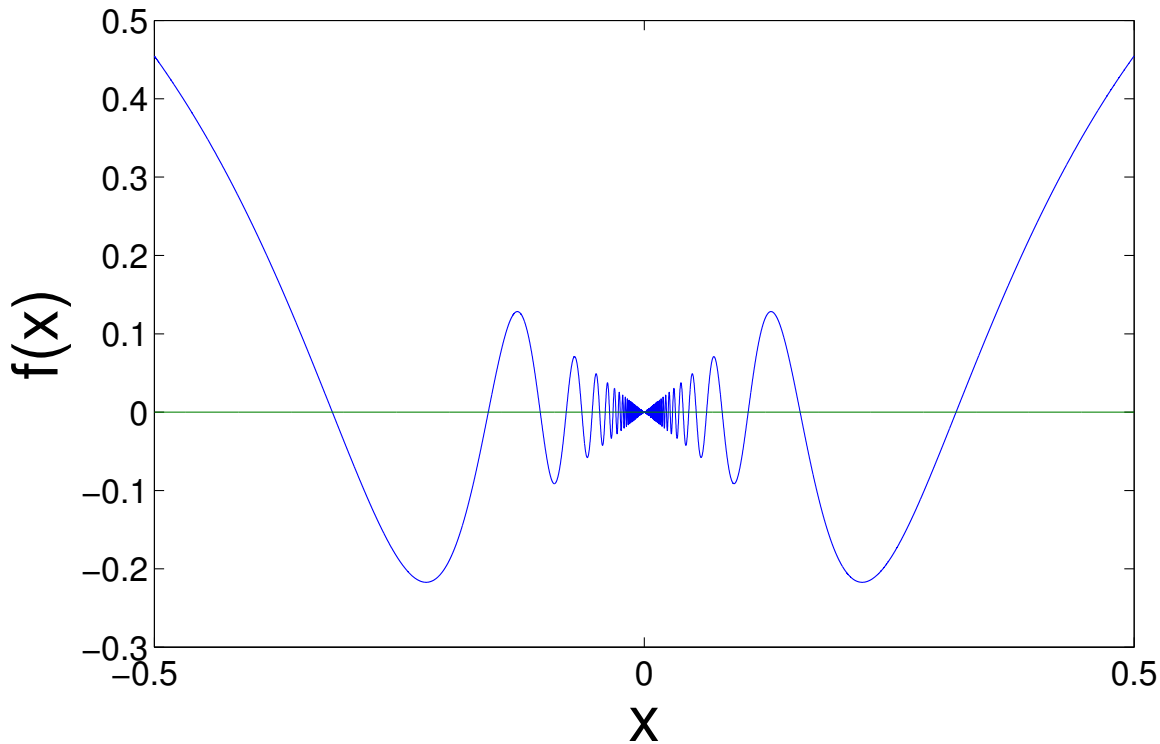
$$f(x) = 0, \quad \forall x \in \mathbb{R}$$

Results

Theorem 1: The optimal X^* is **discrete** with at most finite number of points in any bounded interval.

Outline of proof:

- Proof by contradiction.

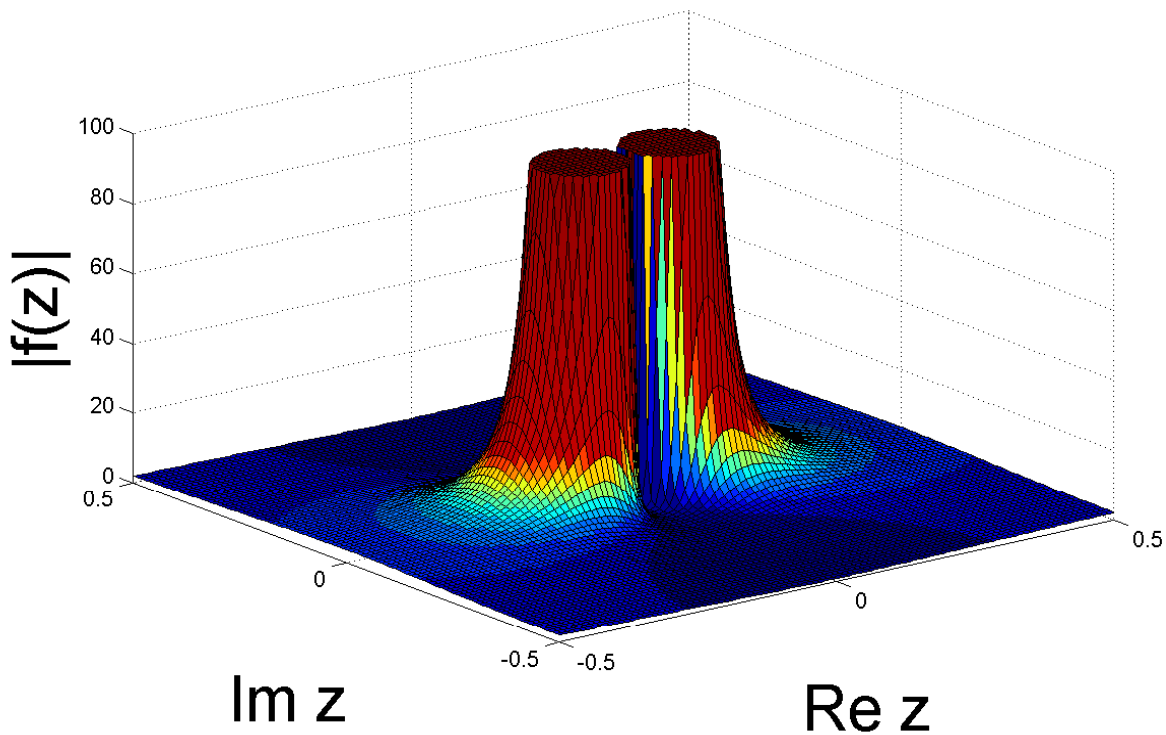


Results

Theorem 1: The optimal X^* is **discrete** with at most finite number of points in any bounded interval.

Outline of proof:

- Proof by contradiction.



Results

Theorem 1: The optimal X^* is **discrete** with at most finite number of points in any bounded interval.

Outline of proof:

- Proof by contradiction.
- Recall the KKT conditions:

$$\begin{aligned} f(x) \geq & 0, \quad \forall x \in \mathbb{R} \\ f(x) = & 0, \quad x \in E = \operatorname{supp} X^* \end{aligned}$$

- Assume E contains infinitely many points with a converging subsequence.
- Observe that f extends analytically to the complex plane.
- Using the *Identity theorem*, conclude that

$$f(x) = 0, \quad \forall x \in \mathbb{R}$$

- Simplify and use Laplace transform along with other bounds on $p(y)$ to yield the contradiction.

More results

Theorem 2: The support of X^* has **finite** number of mass points.

More results

Theorem 2: The support of X^* has **finite** number of mass points.

Outline of proof:

More results

Theorem 2: The support of X^* has **finite** number of mass points.

Outline of proof:

- Proof by contradiction.

More results

Theorem 2: The support of X^* has **finite** number of mass points.

Outline of proof:

- Proof by contradiction.
- Observe continuous differentiability of $f(x)$.

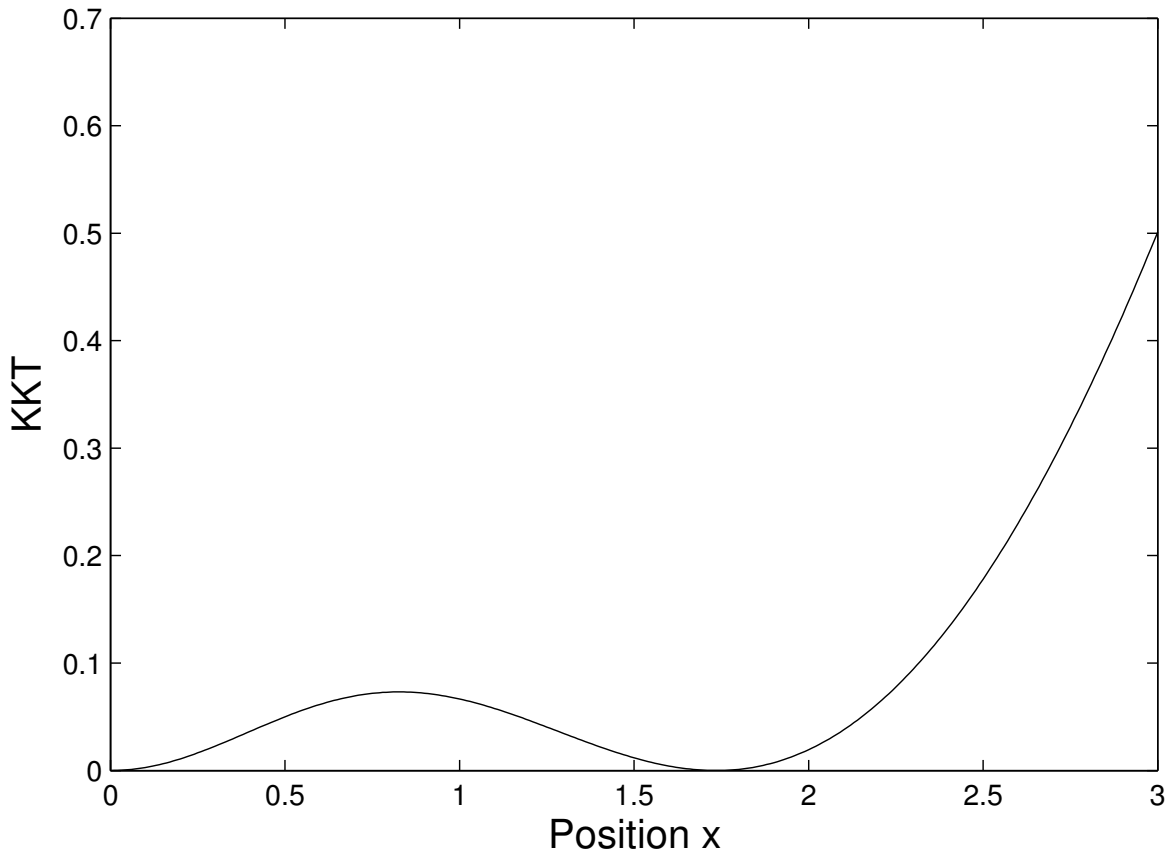
More results

Theorem 2: The support of X^* has **finite** number of mass points.

Outline of proof:

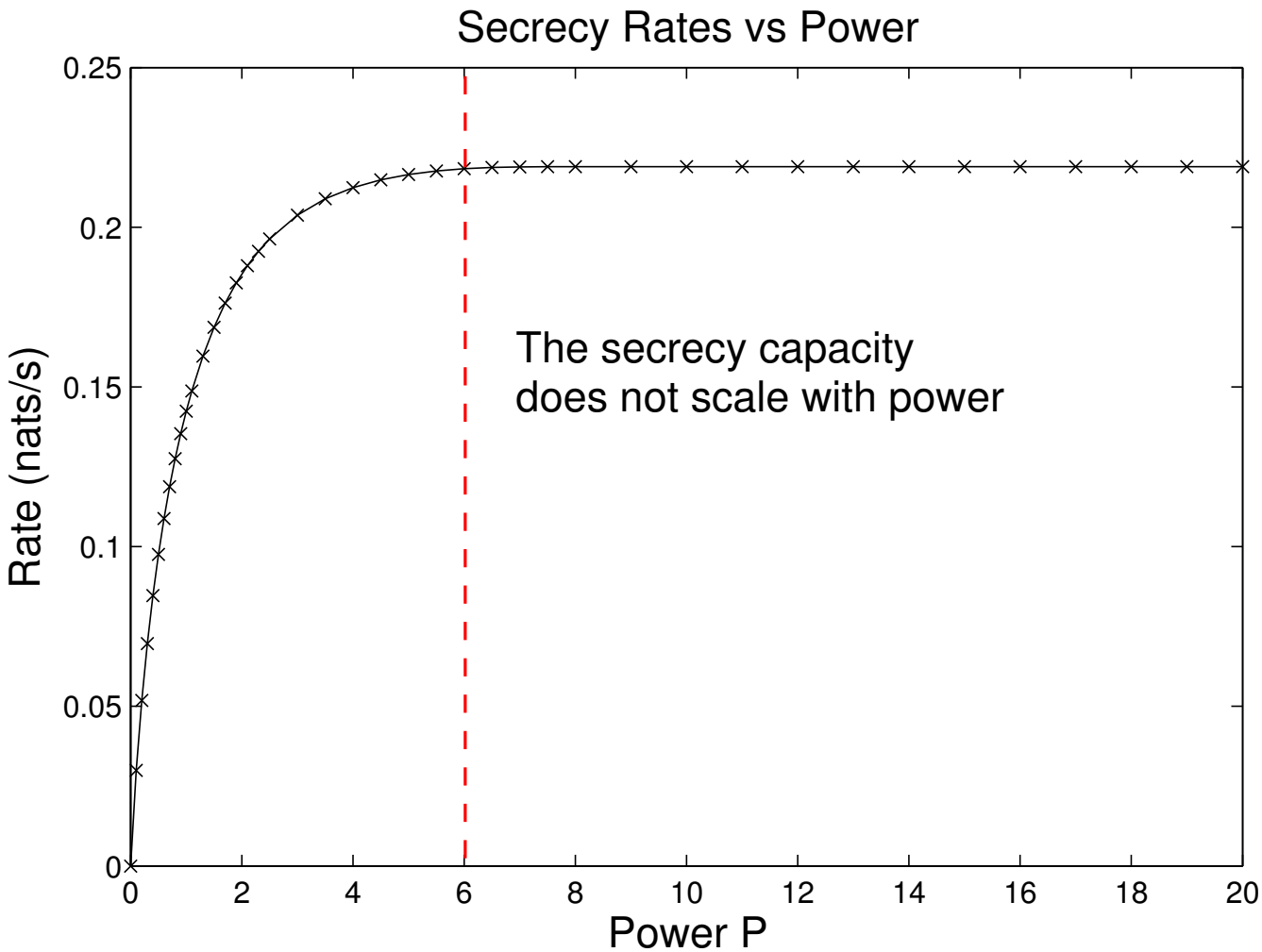
- Proof by contradiction.
- Observe continuous differentiability of $f(x)$.
- Analyse $f'(x)$ and use other bounds on $p(y)$ to reach a contradiction.

Numerical results



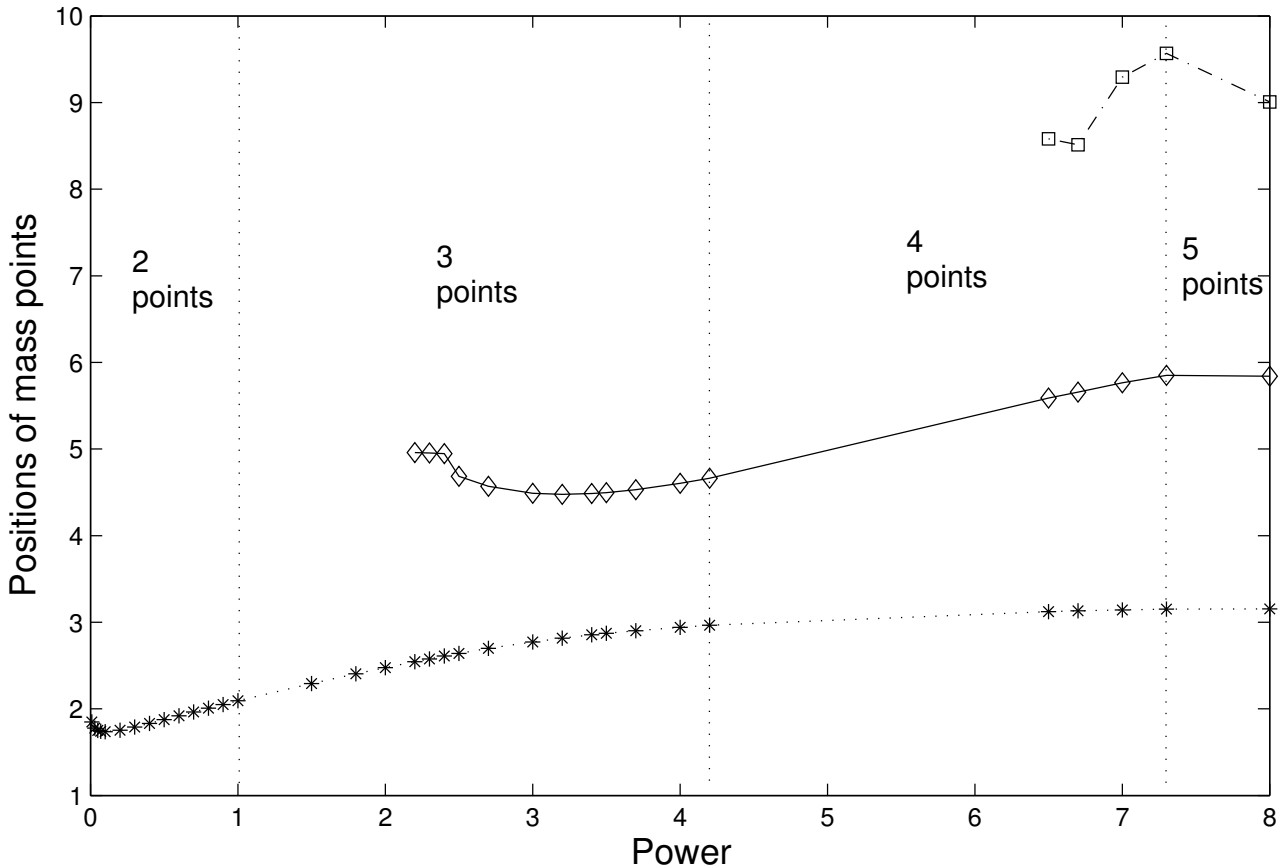
Satisfying the KKT conditions with $P = 0.1$, $\sigma_h = \sigma_1 = 1$, $\sigma_2 = 2$, $\gamma = 0.2461$, $C_s = 0.03$ and $F(x) = 0.9668\delta(x) + 0.0332\delta(x - 1.7348)$.

Numerical results



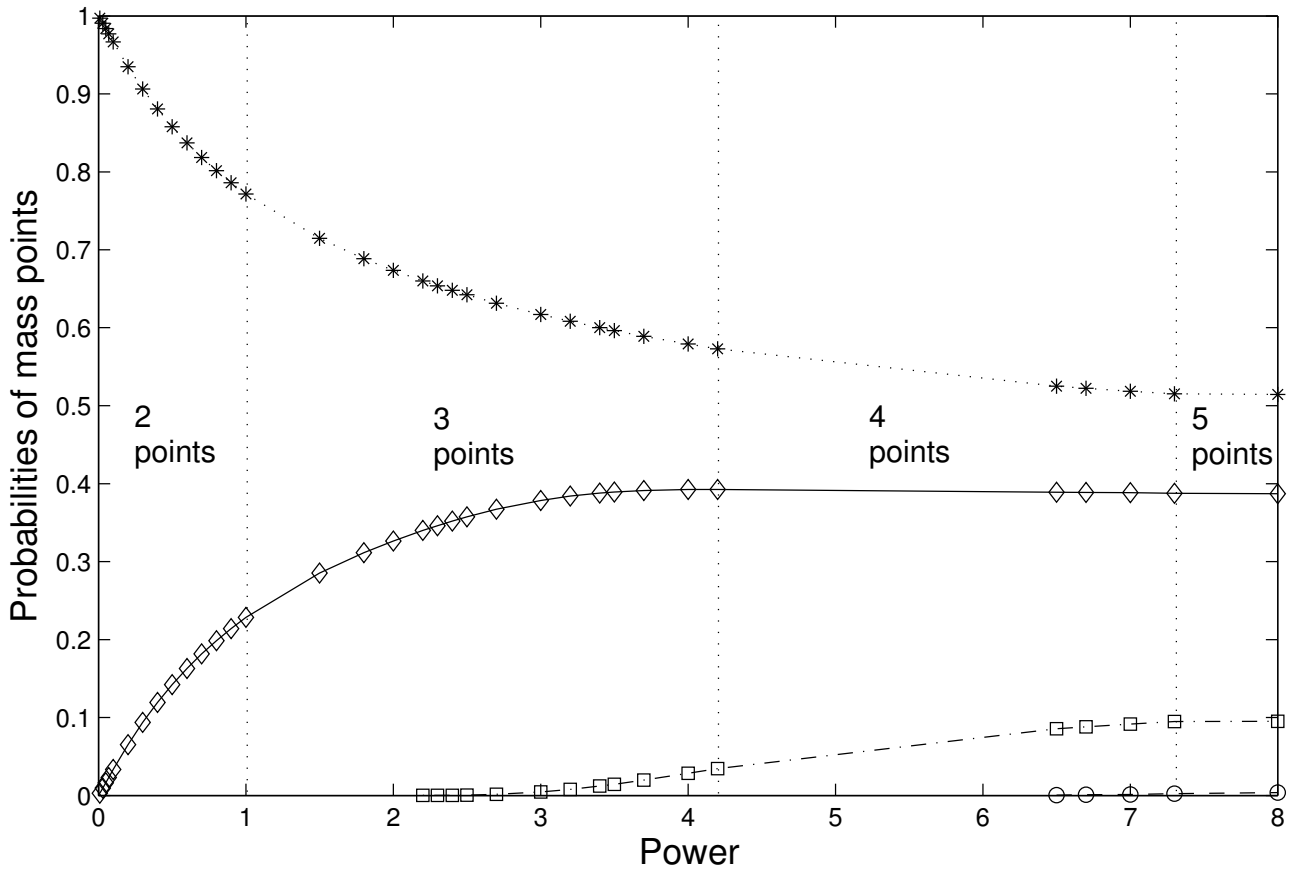
Secrecy capacity versus power.

Numerical results



The position of the mass points versus power.

Numerical results



The probabilities of the mass points versus power.

Conclusions

- Studied the Rayleigh fast fading wiretap channel with coherence time 1 and no CSI anywhere.

Conclusions

- Studied the Rayleigh fast fading wiretap channel with coherence time 1 and no CSI anywhere.
- Proved that the optimal input distribution is discrete with finite number of mass points.