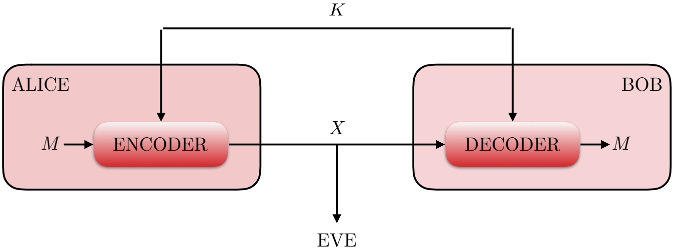
3. Shannon's Secrecy System

Outline

3. Shannon's Secrecy System

- Coding scheme
- Perfect secrecy
- Crypto lemma
- One-time pad

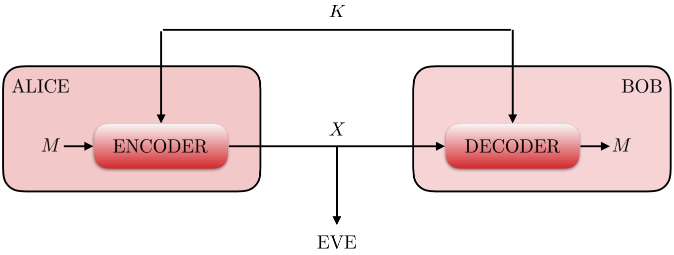
Shannon's Secrecy System



- Shannon proposed the idea of measuring quantitatively the secrecy level of encryption systems
- Shannon's model is often called *Shannon's secrecy system* or *Shannon's cypher system*

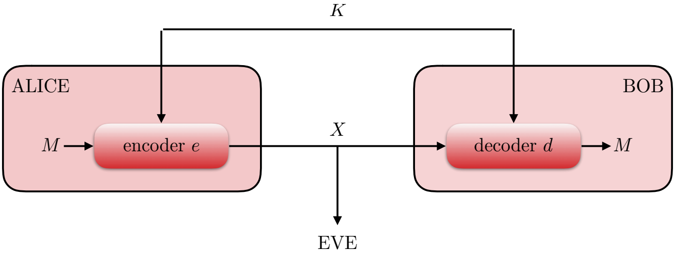
C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949

Shannon's Secrecy System (2)



- Transmitter (Alice) communicates with a legitimate receiver (Bob) over a noiseless channel, while an eavesdropper (Eve) overhears all signals sent over the channel
- To prevent Eve from retrieving any information, Alice encodes her messages into codewords by means of a secret key, which is **known** to Bob, but **unknown** to Eve

Coding Scheme



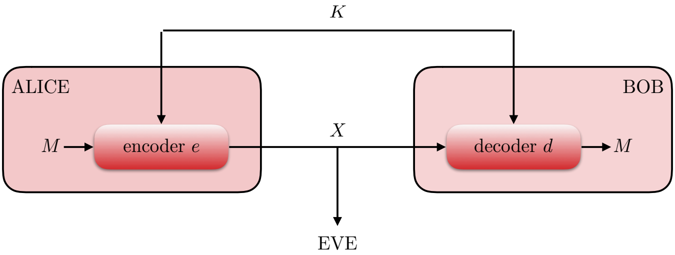
- Quantities represented by random variables
  - messages $M \in \mathcal{M}$
  - codewords $X \in \mathcal{X}$
  - secret keys $K \in \mathcal{K}$

- Encoder e and and decoder d are functions

$$e : \mathcal{M} \times \mathcal{K} \to \mathcal{X} \quad \text{and} \quad d : \mathcal{X} \times \mathcal{K} \to \mathcal{M}$$

➠ The pair (e, d) is called *coding scheme*

Coding Scheme (2)



- The legitimate receiver is assumed to *retrieve message without error*, i.e.,

$$M = d(X, K) \quad \text{and} \quad X = e(M, K)$$

- Although Eve has no knowledge about the secret key K, she is assumed to know the **encoding function** e and **the decoding function** d

Perfect Secrecy

- Secrecy is measured in terms of the conditional entropy $H(M|X)$, which we call eavesdropper's *equivocation*
- Intuitively, equivocation represents Eve's uncertainty about the messages after incepting the codewords
- A coding scheme achieves *perfect secrecy* if

$$\boldsymbol{H(M|X) = H(M)} \quad \text{or, equivalently,} \quad \boldsymbol{I(M;X) = 0}$$

- We call $I(M;X)$ the *leakage of information* to the eavesdropper
- In other words, perfect secrecy is achieved if codewords X are statistically independent of messages M
- This differs from the traditional assessment based on computational complexity: it provides a *quantitative* metric to measure secrecy and it disregards the computational power of Eve
- Perfect secrecy guarantees that Eve's optimal attack is to **guess the message M at random** and that **there exists no algorithm that could extract any information about M from X**

Perfect Secrecy

- Secrecy is measured in terms of the conditional entropy $H(M|X)$, which we call eavesdropper's *equivocation*
- Intuitively, equivocation represents Eve's uncertainty about the messages after incepting the codewords
- A coding scheme achieves *perfect secrecy* if

$$\boldsymbol{H(M|X) = H(M)} \quad \text{or, equivalently,} \quad \boldsymbol{I(M;X) = 0}$$

- We call $I(M;X)$ the *leakage of information* to the eavesdropper
- In other words, perfect secrecy is achieved if codewords X are statistically independent of messages M
- This differs from the traditional assessment based on computational complexity: it provides a *quantitative* metric to measure secrecy and it disregards the computational power of Eve
- Perfect secrecy guarantees that Eve's optimal attack is to **guess the message M at random** and that **there exists no algorithm that could extract any information about M from X**

Perfect Secrecy

- Secrecy is measured in terms of the conditional entropy $H(M|X)$, which we call eavesdropper's *equivocation*
- Intuitively, equivocation represents Eve's uncertainty about the messages after incepting the codewords
- A coding scheme achieves *perfect secrecy* if

$$\boldsymbol{H(M|X) = H(M)} \quad \text{or, equivalently,} \quad \boldsymbol{I(M;X) = 0}$$

- We call $I(M;X)$ the *leakage of information* to the eavesdropper
- In other words, perfect secrecy is achieved if codewords X are statistically independent of messages M
- This differs from the traditional assessment based on computational complexity: it provides a *quantitative* metric to measure secrecy and it disregards the computational power of Eve
- Perfect secrecy guarantees that Eve's optimal attack is to **guess the message M at random** and that **there exists no algorithm that could extract any information about M from X**

Perfect Secrecy (2)

Proposition

If a coding scheme for Shannon's secrecy system achieves perfect secrecy, then

$$\boldsymbol{H(K) \geq H(M)}.$$

Proof:

- Consider a coding scheme that achieves perfect secrecy; then by assumption

$$H(M|X) = H(M)$$

- In addition, since messages M are decoded without errors upon observing X and K, *Fano's inequality* ensures that

$$H(M|X, K) = 0$$

Perfect Secrecy (2)

Proposition

If a coding scheme for Shannon's secrecy system achieves perfect secrecy, then

$$\boldsymbol{H(K) \geq H(M)}.$$

Proof:

- Consider a coding scheme that achieves perfect secrecy; then by assumption

$$H(M|X) = H(M)$$

- In addition, since messages M are decoded without errors upon observing X and K, *Fano's inequality* ensures that

$$H(M|X, K) = 0$$

Perfect Secrecy (2)

Proposition

If a coding scheme for Shannon's secrecy system achieves perfect secrecy, then

$$\boldsymbol{H(K) \geq H(M)}.$$

Proof:

- Consider a coding scheme that achieves perfect secrecy; then by assumption
$$H(M|X) = H(M)$$
- In addition, since messages M are decoded without errors upon observing X and K, *Fano's inequality* ensures that
$$H(M|X, K) = 0$$

Perfect Secrecy (3)

- We have

$$
\begin{aligned}
H(K) &\geq H(K) - H(K|X,M) && \text{(since } H(K|X,M) \geq 0\text{)} \\
&\geq H(K|X) - H(K|X,M) && \text{(conditioning reduces entropy)} \\
&= I(K;M|X) \\
&= H(M|X) - H(M|K,X) \\
&= H(M|X) && \text{(Fano's inequality)} \\
&= H(M) && \text{(prefect secrecy)}
\end{aligned}
$$

$\square$

Perfect Secrecy (3)

- We have

$$
\begin{aligned}
H(K) &\geq H(K) - H(K|X,M) && \text{(since } H(K|X,M) \geq 0\text{)} \\
&\geq H(K|X) - H(K|X,M) && \text{(conditioning reduces entropy)} \\
&= I(K;M|X) \\
&= H(M|X) - H(M|K,X) \\
&= H(M|X) && \text{(Fano's inequality)} \\
&= H(M) && \text{(prefect secrecy)}
\end{aligned}
$$

$\square$

Perfect Secrecy (3)

- We have

$$
\begin{aligned}
H(K) &\geq H(K) - H(K|X,M) && \text{(since } H(K|X,M) \geq 0\text{)}\\
&\geq H(K|X) - H(K|X,M) && \text{(conditioning reduces entropy)}\\
&= I(K;M|X)\\
&= H(M|X) - H(M|K,X)\\
&= H(M|X) && \text{(Fano's inequality)}\\
&= H(M) && \text{(prefect secrecy)}
\end{aligned}
$$

$\square$

Perfect Secrecy (3)

- We have

$$
\begin{aligned}
H(K) &\geq H(K) - H(K|X,M) && \text{(since } H(K|X,M) \geq 0\text{)} \\
&\geq H(K|X) - H(K|X,M) && \text{(conditioning reduces entropy)} \\
&= I(K;M|X) \\
&= H(M|X) - H(M|K,X) \\
&= H(M|X) && \text{(Fano's inequality)} \\
&= H(M) && \text{(prefect secrecy)}
\end{aligned}
$$

$\square$

Perfect Secrecy (3)

- We have

$$
\begin{aligned}
H(K) &\geq H(K) - H(K|X,M) && \text{(since } H(K|X,M) \geq 0\text{)} \\
&\geq H(K|X) - H(K|X,M) && \text{(conditioning reduces entropy)} \\
&= I(K;M|X) \\
&= H(M|X) - H(M|K,X) \\
&= H(M|X) && \text{(Fano's inequality)} \\
&= H(M) && \text{(prefect secrecy)}
\end{aligned}
$$

$\square$

Perfect Secrecy (3)

- We have

$$\begin{aligned}
H(K) &\geq H(K) - H(K|X, M) && \text{(since } H(K|X, M) \geq 0\text{)} \\
&\geq H(K|X) - H(K|X, M) && \text{(conditioning reduces entropy)} \\
&= I(K; M|X) \\
&= H(M|X) - H(M|K, X) \\
&= H(M|X) && \text{(Fano's inequality)} \\
&= H(M) && \text{(prefect secrecy)}
\end{aligned}$$

$\square$

Perfect Secrecy (4)

- Result states that it is **necessary** *to use at least one secret-key bit for each message bit to achieve perfect secrecy*
- If the number of possible messages, keys, and codewords is the same, we obtain a more precise result and establish **necessary and sufficient** conditions for perfect secrecy

Theorem

If $|\mathcal{M}| = |\mathcal{X}| = |\mathcal{K}|$, a coding scheme for Shannon's secrecy system achieves perfect secrecy if and only if

- *for each pair $(m, k) \in \mathcal{M} \times \mathcal{K}$ there exists a unique key $k \in \mathcal{K}$ such that $x = e(m, k)$*
- *the key k is uniformly distributed in $\mathcal{K}$*

Perfect Secrecy (4)

- Result states that it is **necessary** *to use at least one secret-key bit for each message bit to achieve perfect secrecy*
- If the number of possible messages, keys, and codewords is the same, we obtain a more precise result and establish **necessary and sufficient** conditions for perfect secrecy

Theorem

If $|\mathcal{M}| = |\mathcal{X}| = |\mathcal{K}|$, a coding scheme for Shannon's secrecy system achieves perfect secrecy if and only if

- *for each pair $(m, k) \in \mathcal{M} \times \mathcal{K}$ there exists a unique key $k \in \mathcal{K}$ such that $x = e(m, k)$*
- *the key k is uniformly distributed in $\mathcal{K}$*

Perfect Secrecy (5)

Proof:

- First, we prove that conditions are **necessary**:

- Consider coding scheme achieving perfect secrecy with $|\mathcal{M}| = |\mathcal{X}| = |\mathcal{K}|$
- Note that $P_X(x) > 0$ for all $x \in \mathcal{X}$ since otherwise some codewords would never be used and could be removed from $\mathcal{X}$ which would violate the assumption $|\mathcal{M}| = |\mathcal{X}|$
- Since M and X are independent, this implies $P_{X|M}(x|m) = P_X(x) > 0$ for all pairs $(m, x) \in \mathcal{M} \times \mathcal{X}$.
- In other words, for all messages $m \in \mathcal{M}$, the encoder can output all possible codewords in $\mathcal{X}$, thus,

$$\forall m \in \mathcal{M} : \quad \mathcal{X} = \{e(m,k) : k \in \mathcal{K}\}$$

- Because $|\mathcal{X}| = |\mathcal{K}|$, for all $(m, x) \in \mathcal{M} \times \mathcal{X}$ there must be a unique key $k \in \mathcal{K}$ such that $x = e(m, k)$

Perfect Secrecy (5)

Proof:

- First, we prove that conditions are **necessary**:

- Consider coding scheme achieving perfect secrecy with $|\mathcal{M}| = |\mathcal{X}| = |\mathcal{K}|$
- Note that $P_X(x) > 0$ for all $x \in \mathcal{X}$ since otherwise some codewords would never be used and could be removed from $\mathcal{X}$ which would violate the assumption $|\mathcal{M}| = |\mathcal{X}|$
- Since M and X are independent, this implies $P_{X|M}(x|m) = P_X(x) > 0$ for all pairs $(m, x) \in \mathcal{M} \times \mathcal{X}$.
- In other words, for all messages $m \in \mathcal{M}$, the encoder can output all possible codewords in $\mathcal{X}$, thus,

$$\forall m \in \mathcal{M} : \quad \mathcal{X} = \{e(m, k) : k \in \mathcal{K}\}$$

- Because $|\mathcal{X}| = |\mathcal{K}|$, for all $(m, x) \in \mathcal{M} \times \mathcal{X}$ there must be a unique key $k \in \mathcal{K}$ such that $x = e(m, k)$

Perfect Secrecy (5)

Proof:

- First, we prove that conditions are **necessary**:

- Consider coding scheme achieving perfect secrecy with $|\mathcal{M}| = |\mathcal{X}| = |\mathcal{K}|$
- Note that $P_X(x) > 0$ for all $x \in \mathcal{X}$ since otherwise some codewords would never be used and could be removed from $\mathcal{X}$ which would violate the assumption $|\mathcal{M}| = |\mathcal{X}|$
- Since M and X are independent, this implies $P_{X|M}(x|m) = P_X(x) > 0$ for all pairs $(m, x) \in \mathcal{M} \times \mathcal{X}$.
- In other words, for all messages $m \in \mathcal{M}$, the encoder can output all possible codewords in $\mathcal{X}$, thus,

$$\forall m \in \mathcal{M} : \quad \mathcal{X} = \{e(m,k) : k \in \mathcal{K}\}$$

- Because $|\mathcal{X}| = |\mathcal{K}|$, for all $(m, x) \in \mathcal{M} \times \mathcal{X}$ there must be a unique key $k \in \mathcal{K}$ such that $x = e(m, k)$

Perfect Secrecy (6)

- Now, fix an arbitrary codeword $x^* \in \mathcal{X}$. For every message $m \in \mathcal{M}$, let k_m be the unique key such that $x^* = e(m, k_m)$
- Then $P_K(k_m) = P_{X|M}(x^*|m)$ and $\mathcal{K} = \{k_m : m \in \mathcal{M}\}$. Using Bayes' rule, we obtain

$$
\begin{aligned}
P_K(k_m) &= P_{X|M}(x^*|m) \\
&= \frac{P_{M|X}(m|x^*)P_X(x^*)}{P_M(m)} \\
&= P_X(x^*)
\end{aligned}
$$

where the last equality follows from $P_{M|X}(m|x^*) = P_M(m)$ due to independence of M and X

➠ $P_K(k_m)$ takes on the same values for all $m \in \mathcal{M}$ which implies that K is *uniformly distributed in $\mathcal{K}$*

Perfect Secrecy (6)

- Now, fix an arbitrary codeword $x^* \in \mathcal{X}$. For every message $m \in \mathcal{M}$, let k_m be the unique key such that $x^* = e(m, k_m)$
- Then $P_K(k_m) = P_{X|M}(x^*|m)$ and $\mathcal{K} = \{k_m : m \in \mathcal{M}\}$. Using Bayes' rule, we obtain

$$\begin{aligned} P_K(k_m) &= P_{X|M}(x^*|m) \\ &= \frac{P_{M|X}(m|x^*)P_X(x^*)}{P_M(m)} \\ &= P_X(x^*) \end{aligned}$$

where the last equality follows from $P_{M|X}(m|x^*) = P_M(m)$ due to independence of M and X

➠ $P_K(k_m)$ takes on the same values for all $m \in \mathcal{M}$ which implies that K is *uniformly distributed in* $\mathcal{K}$

Perfect Secrecy (6)

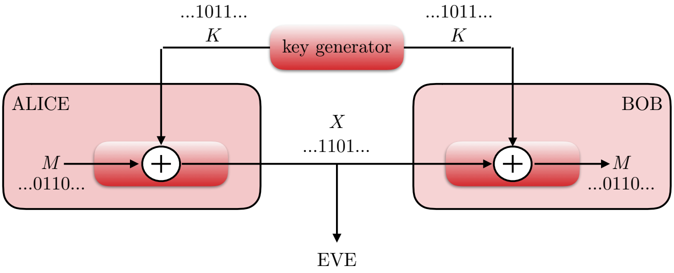
- Now, fix an arbitrary codeword $x^* \in \mathcal{X}$. For every message $m \in \mathcal{M}$, let k_m be the unique key such that $x^* = e(m, k_m)$
- Then $P_K(k_m) = P_{X|M}(x^*|m)$ and $\mathcal{K} = \{k_m : m \in \mathcal{M}\}$. Using Bayes' rule, we obtain

$$\begin{aligned} P_K(k_m) &= P_{X|M}(x^*|m) \\ &= \frac{P_{M|X}(m|x^*)P_X(x^*)}{P_M(m)} \\ &= P_X(x^*) \end{aligned}$$

where the last equality follows from $P_{M|X}(m|x^*) = P_M(m)$ due to independence of M and X

➠ $P_K(k_m)$ takes on the same values for all $m \in \mathcal{M}$ which implies that K is *uniformly distributed in* $\mathcal{K}$

Perfect Secrecy (7)



- Now, we show that the conditions are also **sufficient**
- Since $|\mathcal{M}| = |\mathcal{X}| = |\mathcal{K}|$, we can assume w.l.o.g. that $\mathcal{M} = \mathcal{X} = \mathcal{K} = \{0, 1, 2, ..., |\mathcal{M}| - 1\}$
- Consider a coding scheme shown above which is also called *Vernam cipher* or *one-time pad*
- To send a message $m \in \mathcal{M}$, Alice transmits $x = m \oplus k$ with k is the realization of a key K, which is independent of the message and uniformly distributed on $\mathcal{M}$ and $\oplus$ is the modulo-$|\mathcal{M}|$ addition

Perfect Secrecy (8)

- Since k is known to Bob, he can decode the message m from the codeword x without error by computing

$$x \oplus k = m \oplus k \ominus k = m$$

where $\ominus$ is the modulo-$|\mathcal{M}|$ subtraction

- In addition, this guarantees that for all $x \in \mathcal{X}$

$$P_X(x) = \sum_{k \in \mathcal{M}} P_{X|K}(x|k) P_K(k) = \sum_{k \in \mathcal{M}} P_M(x \oplus k) \frac{1}{|\mathcal{M}|} = \frac{1}{|\mathcal{M}|}$$

and consequently

$$\begin{aligned} I(M;X) &= H(X) - H(X|M) \\ &= H(X) - H(K|M) \quad \text{(one-to-one mapping between } X \text{ and } K\text{)} \\ &= H(X) - H(K) \quad (M \text{ and } K \text{ are independent}) \\ &= \log|\mathcal{M}| - \log|\mathcal{M}| = 0 \end{aligned}$$

- Note that this result holds for any probability distribution of the message P_M for which $\forall m \in \mathcal{M} : P_M(m) > 0$ $\square$

Perfect Secrecy (8)

- Since k is known to Bob, he can decode the message m from the codeword x without error by computing

$$x \oplus k = m \oplus k \ominus k = m$$

  where $\ominus$ is the modulo-$|\mathcal{M}|$ subtraction
- In addition, this guarantees that for all $x \in \mathcal{X}$

$$P_X(x) = \sum_{k \in \mathcal{M}} P_{X|K}(x|k) P_K(k) = \sum_{k \in \mathcal{M}} P_M(x \oplus k) \frac{1}{|\mathcal{M}|} = \frac{1}{|\mathcal{M}|}$$

  and consequently

$$\begin{aligned} I(M;X) &= H(X) - H(X|M) \\ &= H(X) - H(K|M) \quad \text{(one-to-one mapping between } X \text{ and } K\text{)} \\ &= H(X) - H(K) \quad (M \text{ and } K \text{ are independent}) \\ &= \log|\mathcal{M}| - \log|\mathcal{M}| = 0 \end{aligned}$$

- Note that this result holds for any probability distribution of the message P_M for which $\forall m \in \mathcal{M} : P_M(m) > 0$ □

Perfect Secrecy (8)

- Since k is known to Bob, he can decode the message m from the codeword x without error by computing

$$x \oplus k = m \oplus k \ominus k = m$$

where $\ominus$ is the modulo-$|\mathcal{M}|$ subtraction

- In addition, this guarantees that for all $x \in \mathcal{X}$

$$P_X(x) = \sum_{k \in \mathcal{M}} P_{X|K}(x|k) P_K(k) = \sum_{k \in \mathcal{M}} P_M(x \oplus k) \frac{1}{|\mathcal{M}|} = \frac{1}{|\mathcal{M}|}$$

and consequently

$$\begin{aligned} I(M;X) &= H(X) - H(X|M) \\ &= H(X) - H(K|M) && \text{(one-to-one mapping between } X \text{ and } K\text{)} \\ &= H(X) - H(K) && (M \text{ and } K \text{ are independent}) \\ &= \log|\mathcal{M}| - \log|\mathcal{M}| = 0 \end{aligned}$$

- Note that this result holds for any probability distribution of the message P_M for which $\forall m \in \mathcal{M} : P_M(m) > 0$ □

Perfect Secrecy (8)

- Since k is known to Bob, he can decode the message m from the codeword x without error by computing

$$x \oplus k = m \oplus k \ominus k = m$$

where $\ominus$ is the modulo-$|\mathcal{M}|$ subtraction

- In addition, this guarantees that for all $x \in \mathcal{X}$

$$P_X(x) = \sum_{k \in \mathcal{M}} P_{X|K}(x|k) P_K(k) = \sum_{k \in \mathcal{M}} P_M(x \oplus k) \frac{1}{|\mathcal{M}|} = \frac{1}{|\mathcal{M}|}$$

and consequently

$$\begin{aligned} I(M;X) &= H(X) - H(X|M) \\ &= H(X) - H(K|M) \quad \text{(one-to-one mapping between } X \text{ and } K\text{)} \\ &= H(X) - H(K) \quad (M \text{ and } K \text{ are independent}) \\ &= \log|\mathcal{M}| - \log|\mathcal{M}| = 0 \end{aligned}$$

- Note that this result holds for any probability distribution of the message P_M for which $\forall m \in \mathcal{M} : P_M(m) > 0$ □

Perfect Secrecy (8)

- Since k is known to Bob, he can decode the message m from the codeword x without error by computing

$$x \oplus k = m \oplus k \ominus k = m$$

where $\ominus$ is the modulo-$|\mathcal{M}|$ subtraction

- In addition, this guarantees that for all $x \in \mathcal{X}$

$$P_X(x) = \sum_{k \in \mathcal{M}} P_{X|K}(x|k) P_K(k) = \sum_{k \in \mathcal{M}} P_M(x \oplus k) \frac{1}{|\mathcal{M}|} = \frac{1}{|\mathcal{M}|}$$

and consequently

$$\begin{aligned} I(M;X) &= H(X) - H(X|M) \\ &= H(X) - H(K|M) \quad \text{(one-to-one mapping between } X \text{ and } K\text{)} \\ &= H(X) - H(K) \quad (M \text{ and } K \text{ are independent}) \\ &= \log|\mathcal{M}| - \log|\mathcal{M}| = 0 \end{aligned}$$

- Note that this result holds for any probability distribution of the message P_M for which $\forall m \in \mathcal{M} : P_M(m) > 0$ $\square$

Crypto Lemma

- One-time pad guarantees perfect secrecy; so-called "*crypto lemma*"
- Holds under very general conditions (in particular, the finite alphabet $\mathcal{M}$ can be replaced by a compact abelian group $\mathcal{G}$

Lemma (Crypto Lemma)

Let $(\mathcal{G}, +)$ be a compact abelian group with binary operation $+$ and let $X = M + K$ where M and K are random variables over $\mathcal{G}$ and K is independent of M and uniform over $\mathcal{G}$. Then X is independent of M and uniform over $\mathcal{G}$.

- Although previous analysis shows existence of coding schemes that achieve perfect secrecy, it is an unsatisfactory result. In fact, since *one-time pad requires a new key bit for each message bit*, it essentially replaces the problem of secure communication by that of secret-key distribution.
- Next, we show that this stems from the absence of noise at the physical layer. In particular, noise affectis Eve's observation

Crypto Lemma

- One-time pad guarantees perfect secrecy; so-called "*crypto lemma*"
- Holds under very general conditions (in particular, the finite alphabet $\mathcal{M}$ can be replaced by a compact abelian group $\mathcal{G}$

Lemma (Crypto Lemma)

Let $(\mathcal{G}, +)$ be a compact abelian group with binary operation $+$ and let $X = M + K$ where M and K are random variables over $\mathcal{G}$ and K is independent of M and uniform over $\mathcal{G}$. Then X is independent of M and uniform over $\mathcal{G}$.

- Although previous analysis shows existence of coding schemes that achieve perfect secrecy, it is an unsatisfactory result. In fact, since *one-time pad requires a new key bit for each message bit*, it essentially replaces the problem of secure communication by that of secret-key distribution.
- Next, we show that this stems from the absence of noise at the physical layer. In particular, noise affectis Eve's observation