Perfect secrecy

Last modified: 2026-11-22 19:38:07 (PST)

A cipher hides a message from an eavesdropper who sees only the ciphertext. Mutual information says exactly how much the ciphertext can reveal, and so how much key a cipher needs.

Perfect secrecy

Definition 0.1 (Perfect secrecy)**.** Let M be a message, let K be a key independent of M, and let C be the ciphertext made from M and K, all discrete random variables with finite entropies. The key and the ciphertext together determine the message. The cipher has **perfect secrecy** when the ciphertext tells an eavesdropper nothing about the message, that is, when M and C have zero mutual information:

$$\mathbb{I}(M;C) = 0. \tag{1}$$

The definition is from (Shannon 1949).

Example 0.1 (The one-time pad with a two-bit message)**.**
Let the message take the four values $0, 1, 2, 3$ (two bits) with probabilities $0.4, 0.3, 0.2, 0.1$. The key is uniform on the same four values, and the ciphertext is the bitwise exclusive or of message and key. The R chunk below builds the joint distribution of message and ciphertext, and computes the mutual information between them.

```r
prior <- c(0.4, 0.3, 0.2, 0.1)
joint <- matrix(0, nrow = 4, ncol = 4)
for (m in 0:3) {
  for (k in 0:3) {
    c_value <- bitwXor(m, k)
    joint[m + 1, c_value + 1] <- joint[m + 1, c_value + 1] + prior[m + 1] / 4
  }
}
cipher_prob <- colSums(joint)
product <- outer(prior, cipher_prob)
max_gap <- max(abs(joint - product))
mutual_info <- sum(joint * log2(joint / product))
c(max_gap = max_gap, mutual_info = mutual_info)
#>     max_gap mutual_info
#>           0           0
```

The ciphertext is uniform, with probability 0.25 on each value, and the largest gap between the joint distribution and the product of the two marginal distributions is 0. So the mutual information is 0 bits: the pad has perfect secrecy for these message probabilities.

Theorem 0.1 (Perfect secrecy needs a key with at least the entropy of the message)**.** *Let M, K and C be as in Definition 0.1, and suppose the cipher has perfect secrecy. Then the entropy of the key is at least the entropy of the message:*

$$\mathbb{H}(K) \geq \mathbb{H}(M). \tag{2}$$

Proof

Proof. By Definition 0.1, $\mathbb{I}(M;C) = 0$, so M and C are independent, and the equality case of conditioning reduces entropy gives the first step:

$$\mathbb{H}(M) = \mathbb{H}(M \mid C). \tag{3}$$

The chain rule expands both conditional entropies below:

$$\mathbb{H}(M \mid C) = \mathbb{H}(M,C) - \mathbb{H}(C), \qquad \mathbb{H}(K \mid C) = \mathbb{H}(K,C) - \mathbb{H}(C). \tag{4}$$

Apply the chain rule to (M,C) and K jointly in two orders:

$$\mathbb{H}(M,C,K) = \mathbb{H}(C,K) + \mathbb{H}(M \mid C,K), \qquad \mathbb{H}(M,C,K) = \mathbb{H}(M,C) + \mathbb{H}(K \mid M,C). \tag{5}$$

The key and the ciphertext determine the message, so $\mathbb{H}(M \mid C, K) = 0$. A conditional entropy is nonnegative, so $\mathbb{H}(K \mid M, C) \geq 0$. Equating the two expansions then gives $\mathbb{H}(M, C) \leq \mathbb{H}(C, K)$. Subtract $\mathbb{H}(C)$ from both sides:

$$\mathbb{H}(M \mid C) \leq \mathbb{H}(K \mid C). \tag{6}$$

By conditioning reduces entropy again, $\mathbb{H}(K \mid C) \leq \mathbb{H}(K)$. Chain the three comparisons:

$$\mathbb{H}(M) = \mathbb{H}(M \mid C) \leq \mathbb{H}(K \mid C) \leq \mathbb{H}(K). \tag{7}$$

□

Example 0.2 (The key of a one-time pad is as long as the message)**.**
The R chunk below computes the entropy of the message and of the key of Example 0.1.

```
prior <- c(0.4, 0.3, 0.2, 0.1)
key_prob <- rep(1 / 4, 4)
message_entropy <- -sum(prior * log2(prior))
key_entropy <- -sum(key_prob * log2(key_prob))
c(message_entropy = message_entropy, key_entropy = key_entropy)
#> message_entropy     key_entropy
#>        1.846439        2.000000
```

The message has 1.846 bits of entropy, and the key has 2 bits, so the key's entropy is at least the message's, as Theorem 0.1 requires. A key with fewer than 1.846 bits of entropy could not give this message perfect secrecy.

Remark 0.1 (Source of the definition and the theorem). Perfect secrecy and the theorem on the key are from (Shannon 1949). The proof above uses only the chain rule and conditioning reduces entropy, both of which are results about entropy.

References

Shannon, C. E. 1949. "Communication Theory of Secrecy Systems." *Bell System Technical Journal* 28 (4): 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x.