

Advantage of authorized receiver over eavesdropper is computational and not information theoretic.

As in all public key encryption schemes the advantage of an authorized receiver over an eavesdropper is a computational advantage and not information theoretic one. The message m is decoded by using the information conveyed by sequences of the transmitted signals, $\mathbf{s}_t^k = (s_t(0), \dots, s_t(k))$ and $\mathbf{s}_r^k = (s_r(0), \dots, s_r(k))$. We show that the amount of information about the message m conveyed by the transmitted coupling signals $\mathbf{s}_r^{T_{bit}}$ and $\mathbf{s}_t^{T_{bit}}$ does not depend on knowledge of the secret dynamics $\mathbf{F}_R(\bullet), G_R(\bullet)$ and state $\mathbf{r}(n)$ of the receiver. As a consequence both authorized and unauthorized receiver have the same amount of information about the transmitted bit.

proof: The mutual information between the message m and the observed transmitted signal sequences $\mathbf{s}_r^{T_{bit}}$ and $\mathbf{s}_t^{T_{bit}}$ is given by

$$\begin{aligned} I(\mathbf{s}_r^{T_{bit}}, \mathbf{s}_t^{T_{bit}}; m) &= H(\mathbf{s}_r^{T_{bit}}, \mathbf{s}_t^{T_{bit}}) - H(\mathbf{s}_r^{T_{bit}}, \mathbf{s}_t^{T_{bit}} | m) \\ &= \sum_{m \in \{0,1\}} \int_{\mathbf{s}_r^{T_{bit}}} \int_{\mathbf{s}_t^{T_{bit}}} p(\mathbf{s}_r^{T_{bit}}, \mathbf{s}_t^{T_{bit}}, m) \cdot \imath(\mathbf{s}_r^{T_{bit}}, \mathbf{s}_t^{T_{bit}}; m) \cdot d\mathbf{s}_r^{T_{bit}} \cdot d\mathbf{s}_t^{T_{bit}} \end{aligned} \quad (1)$$

$$\text{where: } \imath(\mathbf{s}_r^{T_{bit}}, \mathbf{s}_t^{T_{bit}}; m) = -\ln \left(\frac{p(\mathbf{s}_r^{T_{bit}}, \mathbf{s}_t^{T_{bit}})}{p(\mathbf{s}_r^{T_{bit}}, \mathbf{s}_t^{T_{bit}} | m)} \right).$$

The probability $p(\mathbf{s}_r^{T_{bit}}, \mathbf{s}_t^{T_{bit}})$ in Eq.1 can be expanded as

$$\begin{aligned} p(\mathbf{s}_r^{T_{bit}}, \mathbf{s}_t^{T_{bit}}) &= p(s_r(0)) \cdot p(s_t(0) | \mathbf{s}_r^0) \\ &\quad \cdot p(s_r(1) | \mathbf{s}_r^0, \mathbf{s}_t^0) \cdot p(s_t(1) | \mathbf{s}_r^1, \mathbf{s}_t^0) \\ &\quad \vdots \\ &\quad \cdot p(s_r(T_{bit}) | \mathbf{s}_r^{T_{bit}-1}, \mathbf{s}_t^{T_{bit}-1}) \cdot p(s_r(T_{bit}) | \mathbf{s}_r^{T_{bit}}, \mathbf{s}_t^{T_{bit}-1}) \\ &= p(s_r(0)) \cdot p(s_t(0) | \mathbf{s}_r^0) \\ &\quad \cdot \prod_{n=1}^{T_{bit}} \left[p(s_r(n) | \mathbf{s}_r^{n-1}, \mathbf{s}_t^{n-1}) \cdot p(s_t(n) | \mathbf{s}_r^n, \mathbf{s}_t^{n-1}) \right]. \end{aligned} \quad (2)$$

Since $p(s_r(n) | \mathbf{s}_r^{n-1}, \mathbf{s}_t^{n-1}, m)$ depends solely on the dynamics of the receiver, and not on the dynamics of the transmitter it is independent of the parameter m which modulates the dynamics of the transmitter :

$$p(s_r(n) | \mathbf{s}_r^{n-1}, \mathbf{s}_t^{n-1}, m) = p(s_r(n) | \mathbf{s}_r^{n-1}, \mathbf{s}_t^{n-1}). \quad (3)$$

The term $p(s_t(n) | \mathbf{s}_r^n, \mathbf{s}_t^{n-1}, m)$ does depend on the parameter m and we can calculate the probability:

$$\begin{aligned} p(\mathbf{s}_r^{T_{bit}}, \mathbf{s}_t^{T_{bit}} | m) &= p(x(0)) \cdot p(s_t(0) | \mathbf{s}_r^0, m) \\ &\quad \cdot \prod_{n=1}^{T_{bit}} \left[p(s_r(n) | \mathbf{s}_r^{n-1}, \mathbf{s}_t^{n-1}) \cdot p(s_t(n) | \mathbf{s}_r^n, \mathbf{s}_t^{n-1}, m) \right]. \end{aligned} \quad (4)$$

When we substitute Eq. (2) and Eq. (4) into Eq. (1) the terms that depend only on the receiver dynamics and are independent of m (which is part of the transmitter dynamics) cancels, and we have :

$$\imath(m; \mathbf{s}_r^{T_{bit}}, \mathbf{s}_t^{T_{bit}}) = -\ln \frac{p(s_t(0) | s_r(0))}{p(s_t(0) | s_r(0), m)} - \sum_{n=1}^{T_{bit}} \ln \frac{p(s_t(n) | \mathbf{s}_r^n, \mathbf{s}_t^{n-1})}{p(s_t(n) | \mathbf{s}_r^n, \mathbf{s}_t^{n-1}, m)}. \quad (5)$$

The terms in Eq. (5) depend only on the transmitter dynamics $\mathbf{F}_T(\bullet), G_T(\bullet)$ and state $\mathbf{t}(n)$, and do not depend on the receiver dynamics or variables $\mathbf{F}_R(\bullet), G_R(\bullet), \mathbf{r}(n)$. It is evident from substituting Eq. (5) into Eq. (1) that the amount of information about the message m conveyed by the transmitted signals $\mathbf{s}_r^{T_{bit}}$ and $\mathbf{s}_t^{T_{bit}}$ does not depend on the secret dynamics or state of the receiver. The authorized receiver and an eavesdropper have the same amount of information about the transmitted message. However, the position of the dynamical system attractor does depend on the dynamics of the receiver. Even though the position of the attractor does not contain any additional information about the transmitted message, it makes decoding task computationally feasible