Teoría de la Información y Criptografía

Jorge Aziel Rebolledo Araya

Noviembre 2024

Tabla de Contenidos

Motivación

- La dependencia de los sistemas digitales resalta la necesidad de proteger la información.
- La teoría de la información, iniciada por Claude Shannon, ofrece bases matemáticas para optimizar la seguridad criptográfica.
- Este trabajo explora cómo estos principios teóricos se aplican en la práctica.

Palabras Clave

- Entropía de Shannon
- Información mutua
- Seguridad perfecta
- Criptografía simétrica y asimétrica
- Ataques criptográficos
- Capacidad de canal
- Resistencia post-cuántica

Criterios de Búsqueda

- Fuentes: IEEE Xplore, Springer, ScienceDirect, Google Scholar.
- Foco en artículos revisados por pares y libros especializados (2010-2024).
- Temas clave:
  - Relación entre teoría de la información y criptografía.
  - Criptografía post-cuántica.

Resultados Destacados

- **Shannon, C. (1949)**: Fundamentos de la teoría de la información aplicada a la criptografía.
- **Renner, R. (2022)**: Seguridad basada en la teoría de la información en la era cuántica.
- **Bernstein & Lange (2017)**: Análisis de la criptografía post-cuántica.

Relación entre teoría de la información y criptografía

- La entropía mide la incertidumbre de un sistema.
- La información mutua evalúa la dependencia entre dos variables.
- En criptografía:
  - Alta entropía = Sistema menos predecible.
  - Baja información mutua = Mayor resistencia a ataques.

Criptografía Simétrica vs. Asimétrica

- **Simétrica:** Una clave para cifrar y descifrar (ej., AES).
- **Asimétrica:** Pares de claves pública y privada (ej., RSA).

Teoría de la Información en Criptografía

- **Seguridad perfecta:** Ejemplo del One-Time Pad. https://youtu.be/FIIG3TvQCBQ
- **Información mutua:** Cuantifica cuánto se puede inferir de un texto cifrado.
- **Capacidad de canal:** Límite máximo de datos seguros que puede manejar un canal.

Fórmulas de Entropía e Información Mutua

- Entropía (H):

$$H(X) = -\sum_{x \in \mathcal{X}} P(x) \log_2 P(x)$$

  Donde $P(x)$ es la probabilidad de que ocurra un evento x.

- Información mutua (I):

$$I(X;Y) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} P(x,y) \log_2 \frac{P(x,y)}{P(x)P(y)}$$

  La información mutua mide la dependencia entre dos variables aleatorias X e Y.

- Relevancia en One-Time Pad:
  - Para que el cifrado sea perfecto: $I(M;C) = 0$, donde M es el mensaje y C es el cifrado.
  - Esto asegura que no haya fuga de información sobre el mensaje original.

Conclusiones

- La teoría de la información es fundamental en el diseño de sistemas criptográficos.
- Métricas como entropía y capacidad de canal son esenciales para evaluar la seguridad.

Trabajo Futuro

- Investigación en algoritmos criptográficos resistentes a computadoras cuánticas.
- Métodos prácticos para reducir fugas de información en sistemas existentes.

Bibliografía

- Shannon, C. E. *Communication Theory of Secrecy Systems*, 1949.
- Bernstein & Lange. *Post-quantum cryptography*, 2017.
- Renner, R. *Information-Theoretic Security in the Quantum Era*, 2022.