Secure Message Transmission using Noisy Channels and a Shared Key

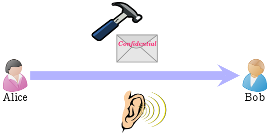
Setareh Sharifian

University of Calgary

April 2020

Secure Communication Problem

Secure communication

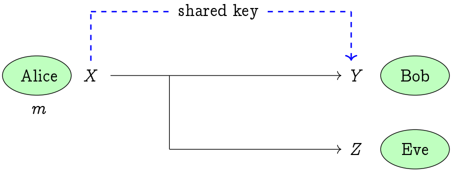


[1] Shannon, Claude E. "Communication theory of secrecy systems."

Secure Communication Problem

Secure communication

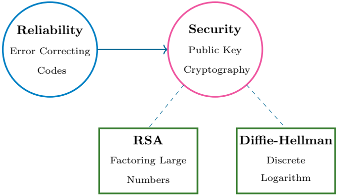
- Reliability & Security?
  - Shannon 1949[1]: the first formal model for secure communication
  - Two steps solution
    - Provide **Reliability**: Error Correcting Codes (ECC)
    - Provide **Security**: One-Time Pad (OTP) with a shared key



[1] Shannon, Claude E. "Communication theory of secrecy systems."

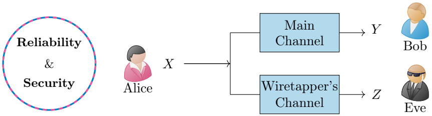
Secure Communication

- Use computational assumptions



Breakable by a quantum computer!

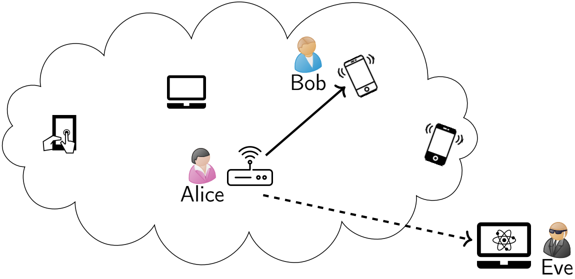
- Use physical assumptions (Information Theoretic)
  - Secure Message Transmission (Wiretap Channel)



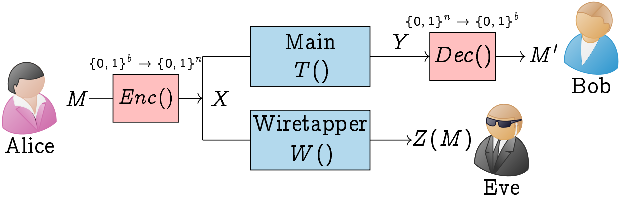
Realizing a Wiretap Channel

An IoT Environment

- Long-term security
- Devices with energy constraints
- Attackers are at longer distances



Message Encoding over Wiretap Channel



- Reliability: $Pr(M \neq M') \leq \sigma_n$
- Strong security[2] **MIS ≡ SS ≡ DS**: $Adv^{xs} \leq \epsilon_n$

$$\textbf{MIS} : \max_{P_M} I(M; Z(M)) = Adv^{mis}$$

$$\textbf{SS} : \max_{f, P_M} [\max_{A} Pr[A(Z) = f(M)] - \max_{s} Pr[S = f(M)] = Adv^{ss}$$

$$\textbf{DS} : \max_{M_0, M_1} SD(Z(M_0); Z(M_1)) = Adv^{ds}$$

- Message transmission rate $R = \frac{b}{n}$

[2] Bellare, Mihir, Stefano Tessaro, and Alexander Vardy. "Semantic security for the wiretap channel."

Secrecy Capacity

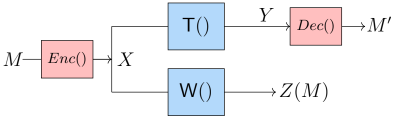
- Secrecy capacity C_s:
  - Highest achievable secure message transmission rate
- C_s for the general channels [CK78]

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

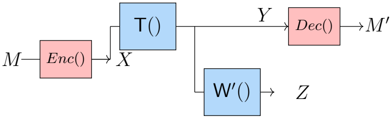
$\Rightarrow$ Secure communication condition: $I(V;Y) > I(V;Z)$

- Explicit C_s
  - (Weakly) Symmetric channels
  - Degraded wiretapper channel

$$C_s = C_\mathsf{T} - C_\mathsf{W}$$



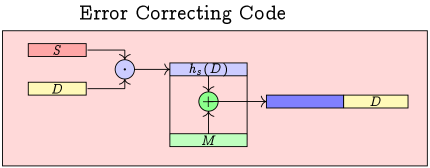
General wiretap channel



Degraded wiretap channel $(X\text{-}Y\text{-}Z)$

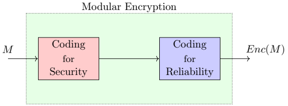
Construction of a WT Encryption System

- HtE: Hash then Encode

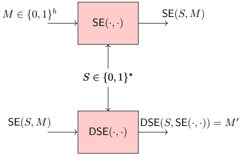


> **Building Block**:efficiently invertible universal hash family (ei-UHF)
>
> – ei-UHF ($g_s(x,y)$) from XoR UHF ($h_s(x)$):
>
> $$g_s(x,y) = h_s(x) \oplus y$$

- Modular Construction



- Seeded Encryption: seed length is amortized asymptotically



XoR UHF: a family of functions $\mathcal{H} = \{h_s | s \in S, h_s : \mathcal{X} \to \mathcal{Y}\}$ for $s \xleftarrow{\$} \mathcal{S}$, where for any $x \neq x' \in \mathcal{X}$ and $a \in \mathcal{Y}$

$$\Pr[h_s(x)_s(x') = a] \leq \frac{1}{|\mathcal{Y}|^2}$$

Security of HtE

- HtE is **SS**≡ **DS** using the framework of [BTV12](for symmetric channels)
  1. Prove **DS** for uniformly random message
  2. Check two properties of the encoding
     - ⋆ Message linear:

$$HtE(\mathbf{k}, \mathbf{s}, \mathbf{m}_1 \oplus \mathbf{m}_2) = HtE(\mathbf{k}, \mathbf{s}, \mathbf{m}_1) \oplus HtE(\mathbf{k}, \mathbf{s}, \mathbf{m}_2)$$

     - ⋆ Separable:

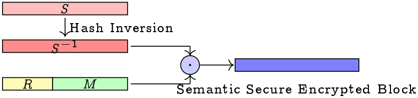
$$HtE(\mathbf{k}, \mathbf{s}, \mathbf{m}) = HtE(\mathbf{k}, \mathbf{s}, 0^b) \oplus HtE(0^k, \mathbf{s}, \mathbf{m})$$

  $\Rightarrow$ **DS** for any message distribution
- Capacity achieving for degraded WT channels with symmetric channels
  - Seed length is amortized asymptotically

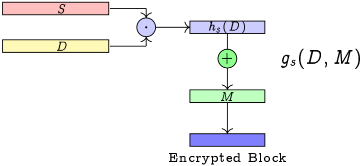
Finite-length Comparison of HtE and ItE

We only look at the secure coding block

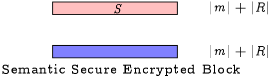
ItE: Invert then Encode [BTV12]



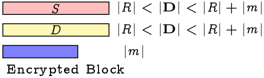
HtE: Hash then Encode



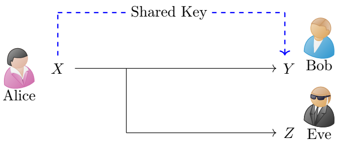
Transmitted Blocks:



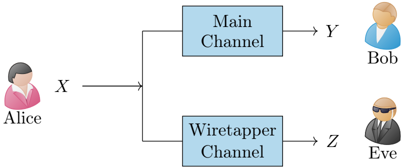
Transmitted Blocks:



Shannon vs Wyner



Shannon Model



Wiretap Model

- Shannon 1949
  - Perfect secrecy requires: $|m| = |k| \Rightarrow$ limited practical applications
- Wyner 1975:
  - Semantic Security is possible at relatively low rate

Shannon + Wyner: Keyed Wiretap Channel

There exist a key K of rate $\mathbf{R}_K = \frac{log|\mathcal{K}|}{n}$ over the wiretap channel

- **Theorem**[3]: The secrecy capacity of the general wiretap channel with a shared key of rate $\mathbf{R}_K$

$$\max_{V \to X \to YZ} \min\left([I(V;Y) - I(V;Z)]^+ + \mathbf{R}_K, I(V;Y)\right)$$

[3] Kang, Wei, and Nan Liu. "Wiretap channel with shared key."

Shannon + Wyner: Keyed Wiretap Channel

There exist a key K of rate $\mathbf{R}_K = \frac{log|\mathcal{K}|}{n}$ over the wiretap channel

- **Theorem**[3]: The secrecy capacity of the general wiretap channel with a shared key of rate $\mathbf{R}_K$

$$\max_{V \to X \to YZ} \min\left([I(V;Y) - I(V;Z)]^+ + \mathbf{R}_K, I(V;Y)\right)$$

[3] Kang, Wei, and Nan Liu. "Wiretap channel with shared key."

Shannon + Wyner: Keyed Wiretap Channel

There exist a key K of rate $\mathbf{R}_K = \frac{log|\mathcal{K}|}{n}$ over the wiretap channel

- **Theorem**[3]: The secrecy capacity of the general wiretap channel with a shared key of rate $\mathbf{R}_K$

$$\max_{V \to X \to YZ} \min \left([I(V;Y) - I(V;Z)]^+ + \mathbf{R}_K, I(V;Y) \right)$$

- Security is in terms of normalized mutual information for uniform message distribution
- Reliability is in terms of average error probability.
- Explicit construction is not given

[3] Kang, Wei, and Nan Liu. "Wiretap channel with shared key."

Shannon + Wyner: Keyed Wiretap Channel

There exist a key K of rate $\mathbf{R}_K = \frac{log|\mathcal{K}|}{n}$ over the wiretap channel

- **Theorem**[3]: The secrecy capacity of the general wiretap channel with a shared key of rate $\mathbf{R}_K$

$$\max_{V \to X \to YZ} \min\left([I(V;Y) - I(V;Z)]^+ + \mathbf{R}_K, I(V;Y)\right)$$

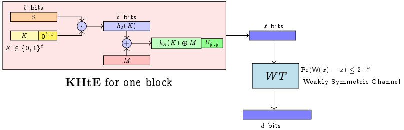
- Security is in terms of ~~normalized mutual information~~ distinguishing advantage for ~~uniform~~ any message distribution
- Reliability is in terms of ~~average~~ maximum error probability.
- Explicit construction is ~~not~~ given

[3] Kang, Wei, and Nan Liu. "Wiretap channel with shared key."

Keyed Wiretap Encoding Schemes

- **KHtE**: Keyed Hash then Encode

ECC:$\{0,1\}^b \rightarrow \{0,1\}^\ell$



KHtE for one block

- Bits that reveal information $\leq d - (\hat{b} - b)$
- Bits that hide information $\leq t + \nu$
  - Key length: $t = n.R_K$
  - Treat the channel as a source of randomness

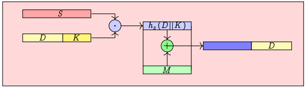
$$\nu = H_\infty(\mathsf{CH}) = -\log\left(\max_{x\in\mathcal{X},y\in\mathcal{Y}} \mathbf{CH}(x,y)\right)$$

- No information leakage $d + b - \hat{b} \approx t + \nu$

$$\mathbf{SD}\left((S, \mathsf{W}(\mathsf{f}(h_S(K)||U_{\hat{b}-b}))); (S, U_\ell)\right) \leq \epsilon.$$

- **KHtE***: The unified code

Error Correcting Code



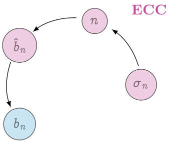
- Becomes HtE when there is no shared key
- Becomes ϵ-One-Time pad when the wiretap's secrecy capacity is zero

Using KHtE in Practice

Theorem 1: **KHtE** is reliable, semantically secure and capacity achieving for weakly degraded wiretap channel with the following choice

$$b_n = n.\mathbf{R}_K + \hat{b}_n - n.\mathbf{C}_{\mathsf{W}} - \sqrt{n}\log(2^\ell + 3).\sqrt{2log\frac{1}{\epsilon_n}} + 2log\epsilon_n$$

- Worst error probability: $\max_{m \in \mathcal{M}} \Pr[(m \neq \hat{m})] < \sigma_n$
- Distingishing security: $2\max_m \mathbf{SD}(\mathsf{W}(\mathsf{Enc}(m)); U_{\mathcal{Z}}) < \epsilon_n$



- Capacity achieving:

$$\mathbf{R} = \lim_{n\to\infty} \frac{b_n}{n} = (\lim_{n\to\infty} \frac{\hat{b}_n}{n} - C_{\mathsf{W}}) + \mathbf{R}_K = C_T - C_W + \mathbf{R}_K$$

Conclusion and Future Works

Concluding Remarks

- An efficient semantically secure wiretap code for DMC wiretap channel
- The *first* semantically secure wiretap code with shared key for weakly symmetric channels
- Finite-length expression for achievable encoding rate

Future Works

- Extending this result to more general channels
- A framework for converting other wiretap codes into the keyed wiretap codes
- Implementation of wiretap codes

Thank You

References I

[BTV12] Mihir Bellare, Stefano Tessaro, and Alexander Vardy, *Semantic security for the wiretap channel*, Advances in Cryptology–CRYPTO 2012, Springer, 2012, pp. 294–311.

[CK78] Imre Csiszár and Janás Körner, *Broadcast channels with confidential messages*, Information Theory, IEEE Transactions on **24** (1978), no. 3, 339–348.

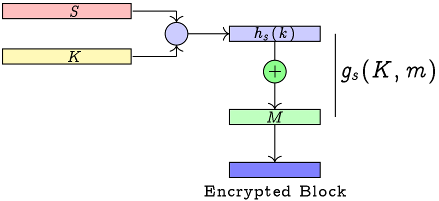
HtE: A Seeded Encryption

- HtE is a modular construction of wiretap codes
  - Semantic secure, capacity achieving, efficient
- ei-UHF is the building block HtE
  - $\mathcal{H} = \{h_s | s \in \mathcal{S}\}$: a family of XoR universal hash functions $\mathcal{X} \rightarrow \mathcal{Y}$

$$g_s(x, y) = h_s(x) \oplus y$$

$\mathcal{G} = \{g_s | s \in \mathcal{S}\}$ is a family of universal hash functions (**ei-UHF**s)

HtE:Hash then Encode



Finite-length Comparison of HtE and ItE

The effective rate of ItE and HtE over a BSC_p with $\sigma = 32$ bits and $p = 0.15, 0.25, 0.35$