A Model for *Adversarial Wiretap Channel*

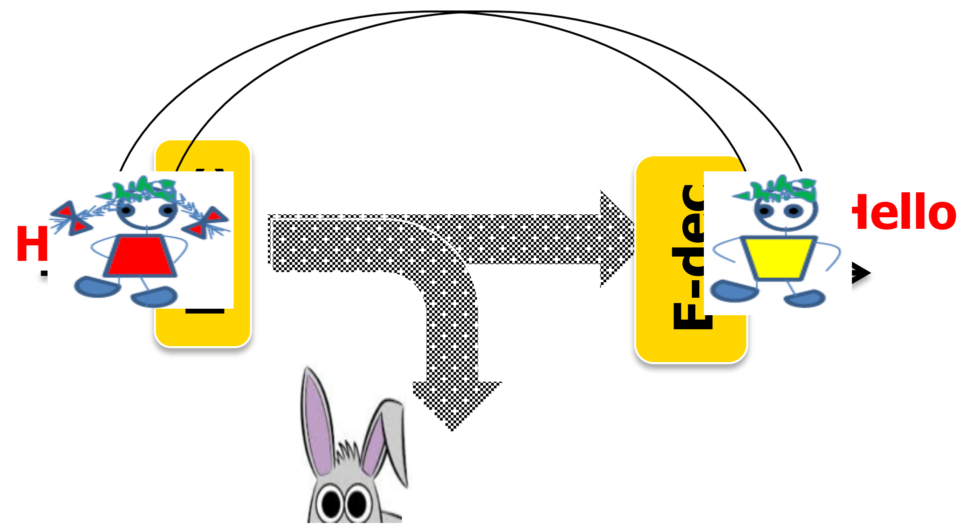
Rei Safavi-Naini, U Calgary, CANADA

Joint work with Pengwei Wang

Alice wants to send a private message to Bob

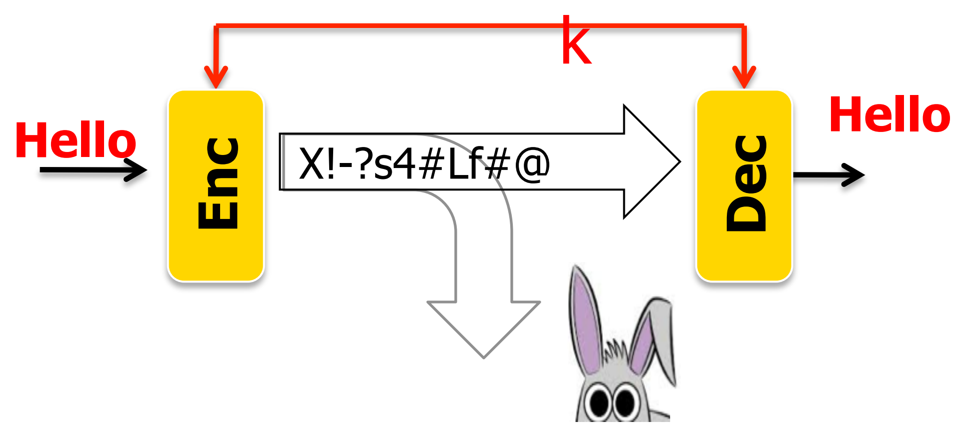
Shannon (1949)

- First reliability



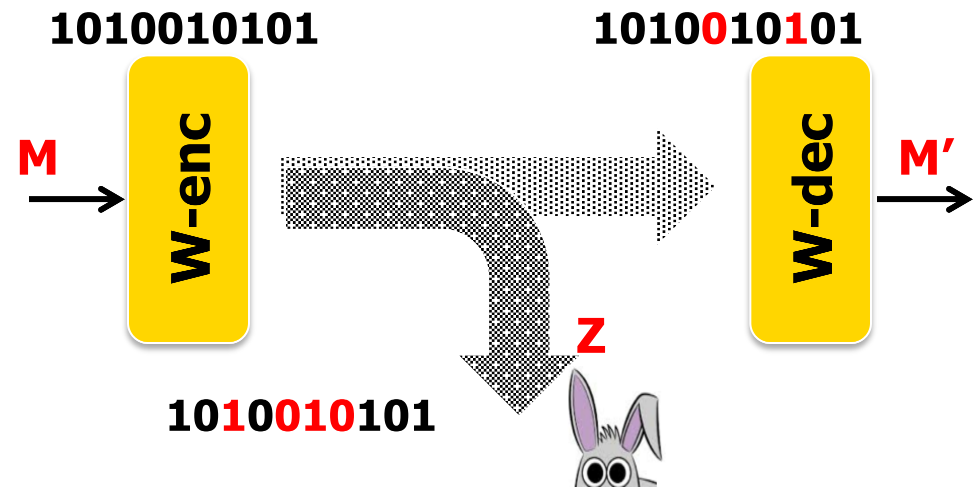
- Then, secrecy

$$H(M \mid Z) = H(M)$$



Alice wants to send a private message to Bob

- Wyner (1975)
- Wiretap channel

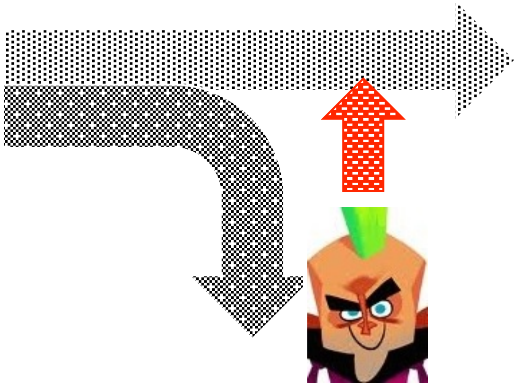


Secrecy: $\frac{1}{k} H(M \mid Z) \geq 1 - \varepsilon$

Reliability: $\Pr(M' \neq M) \leq \varepsilon$

→ *Perfect secrecy*

Adversary

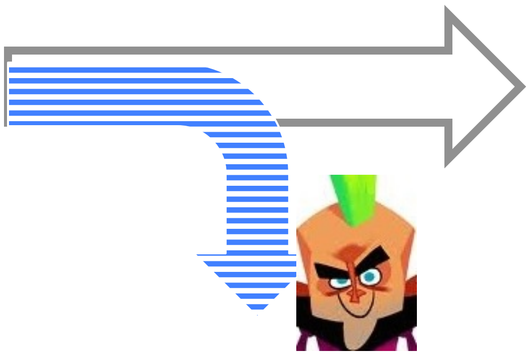


This talk:

- A model for adversarial wiretap
  - Bound & construction
- Relations with other primitives
  1. Networks
  2. Secret Sharing
- Limited View Adversary
  - Reliability
- Concluding remarks

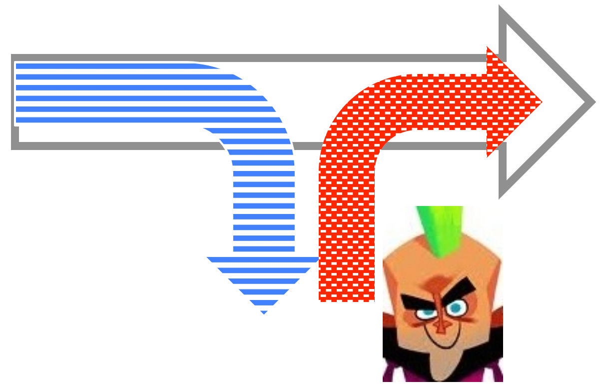
Adversarial Wiretap Channel

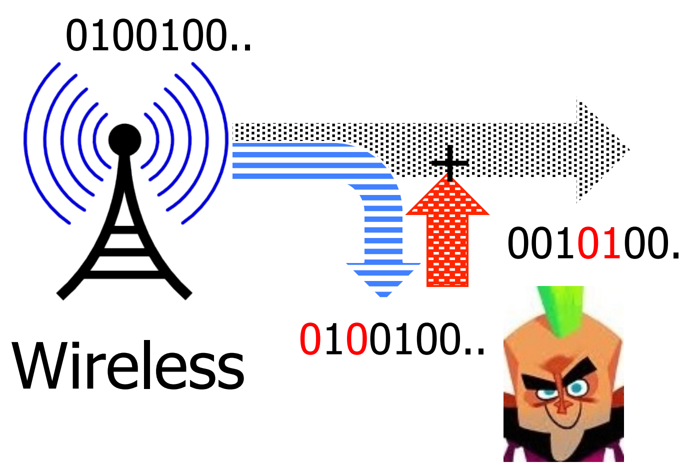
- Wiretap II (OW ‘84)



Adversarial wiretap

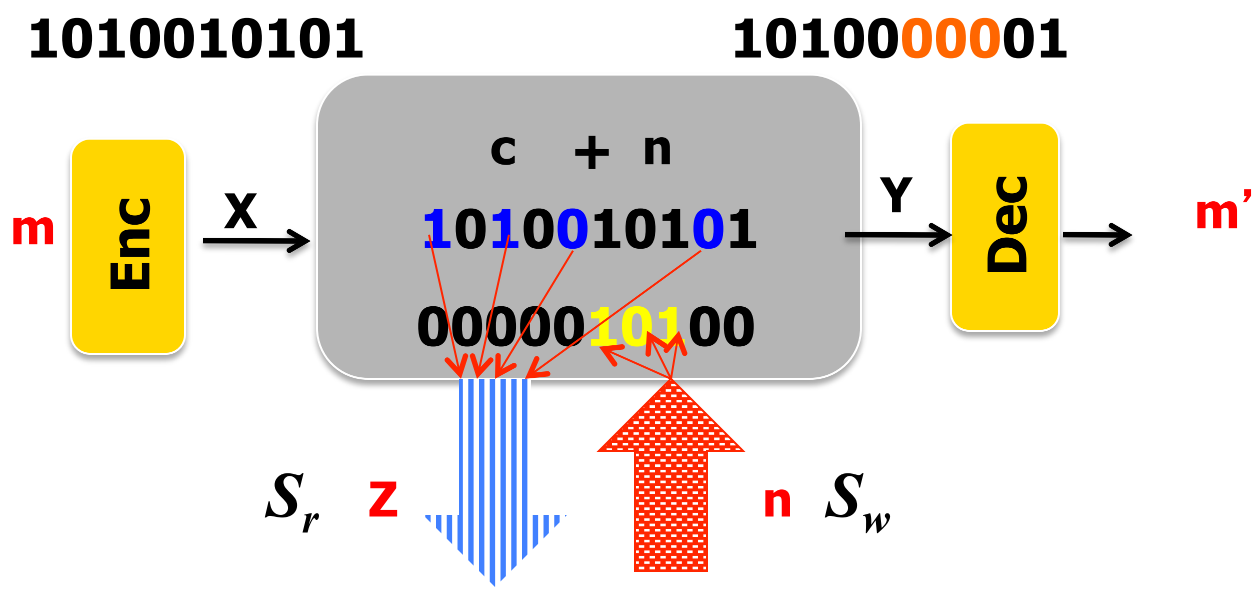
(S-N,W ‘13)





Adversarial Wiretap Channel

Goals: Reliability & Privacy



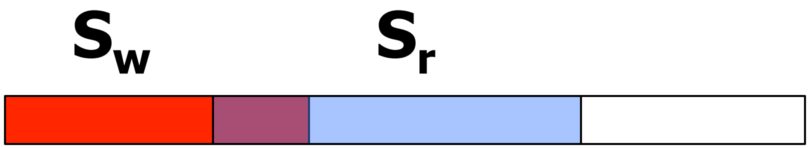
$$|S_r| = \rho_r N, \qquad |S_w| = \rho_w N$$

AWTP Codes

$AWTPenc\ :\ M \times R \rightarrow C \subset \sum^N$ $\qquad$ $AWTPdec\ :\ \sum^N \rightarrow M$

$(\varepsilon, \delta) - AWTP$ code:

- $\Delta(View_A(m_1); View_A(m_2)) \leq \varepsilon$
- $\Pr(M' \neq M) \leq \delta$



$|S_r| = \rho_r N$

$|S_w| = \rho_w N$

$$R(C^N) = \frac{\log|M|}{N \log|\sum|} = \frac{1}{N} \log_{|\sum|} |M|$$

$$\Delta(X;Y) = \frac{1}{2} \sum_i |\Pr(X = i) - \Pr(Y = i)|$$

AWTP Codes

ε***-Code Family*** $\mathbf{C}^{\varepsilon}$: $\{C^N\}_{N \in N}$

$\mathrm{R}(\mathbf{C}^{\varepsilon})$: for any ξ , there exists N_0, such that,

$$\mathrm{N} > \mathrm{N}_0, \qquad \frac{1}{N} \log_{|\Sigma|} |M| \geq \mathrm{R}(\mathbf{C}^{\varepsilon}) - \xi$$

Capacity of a (ρ_r, ρ_w) ***– channel*** :

$$C^{\varepsilon} = \max_{\mathbf{C}^{\varepsilon}} \mathrm{R}(\mathbf{C}^{\varepsilon})$$

$\Rightarrow$ Fraction of a bit that can be sent with perfect reliability, and ε-security.

Upperbound & Capacity

Theorem:

$$C^{\varepsilon} \leq 1 - \rho_r - \rho_w + 2\,\varepsilon\rho_r\,(1 + \log_{|\Sigma|}\frac{1}{\varepsilon})$$

$$C^{0} = 1 - \rho_r - \rho_w$$

$$\rho_r = \rho_w = \rho \Rightarrow 0 \leq C^{0} = 1 - 2\rho$$

$$\Rightarrow \rho \leq \frac{1}{2}$$

Construction

- An *efficient* capacity achieving code

- $\Sigma = F_q$
- Building blocks
  1. AMD codes [CDFPW '08]
  2. Subset evasive sets [DL '11]
  3. Folded Reed-Solomon codes [GD '8]

$$\text{AWTPenc} = FRS(SESenc(AMD(m \| [0]_g)) \| [r]_{u\rho_r L})$$

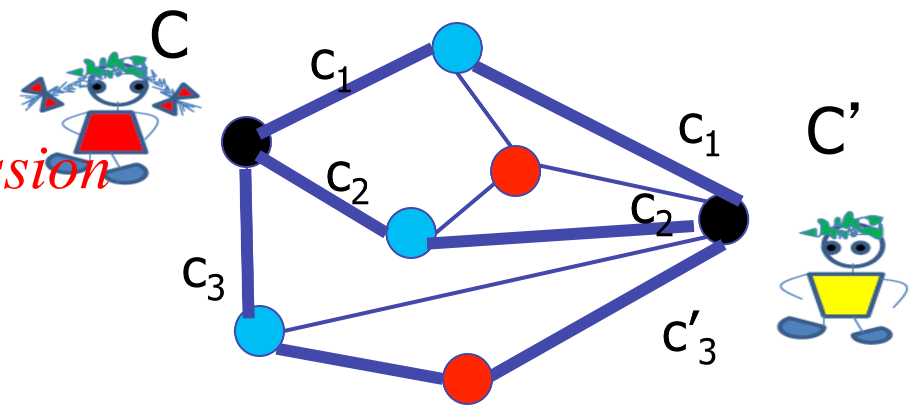
$$\text{AWTPdec} = AMDdec(SESdec(FRSdec(y)))$$

Relation with other primitives

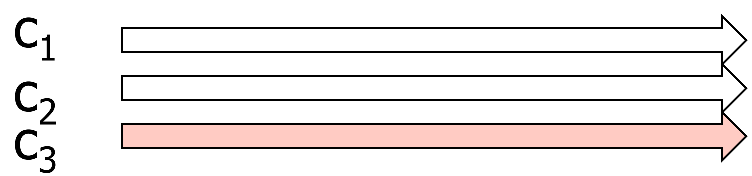
1. Networks
2. Secret Sharing

Relation with other primitives: Security in networks

- DDWY '93, FW '98
- ***Secure Message Transmission***



- *SMTenc(m, r)=C*
- *SMTdec(C')   =m'*



$$(\varepsilon,\delta)-SMT$$

$$\max_{m_1,m_2}\Delta(View_A(m_1,r);View_A(m_2,r))\le\varepsilon$$

Correctness:

$$\forall m\in M,\quad \Pr_R(Dec(C')\ne m)\le\delta$$

Efficiency and Bounds

Corruption

$$N \geq 2t + 1$$

$$1 - \text{round } (0,0)\text{-SMT}:$$

$$N \geq 3t + 1$$

Transmission rate

$$\tau = \frac{\sum_i \log|V_i|}{\log|M|}$$

$$\tau \geq \Omega\left(\frac{N}{N - 2t}\right)$$

AWTP → SMT

- A more general adversary model

- AWTPenc, AWTPdec → (SMTenc, SMTdec)
  - Optimal constructions

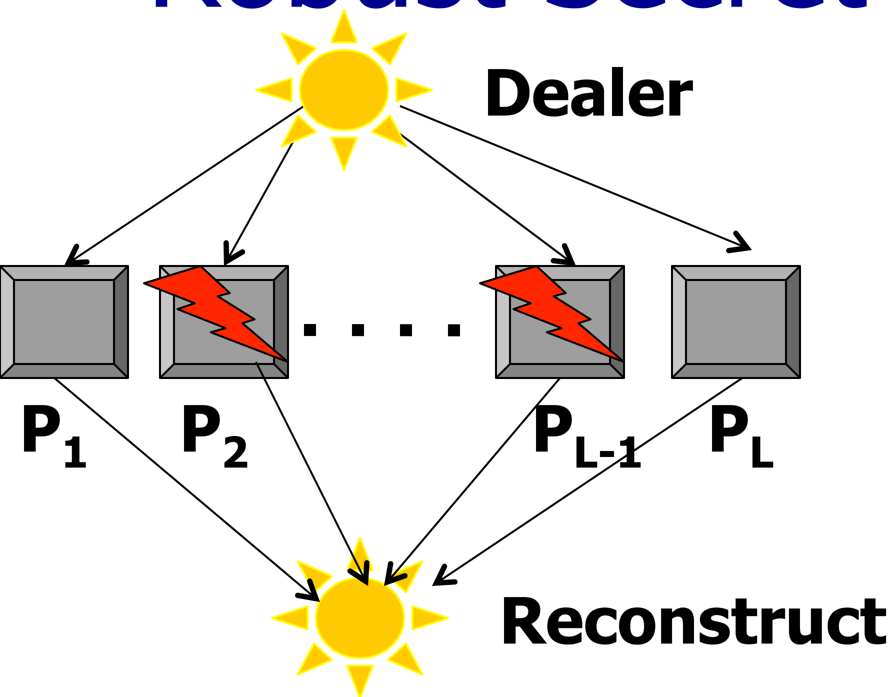
$$\rho_w = \rho_r = \rho$$

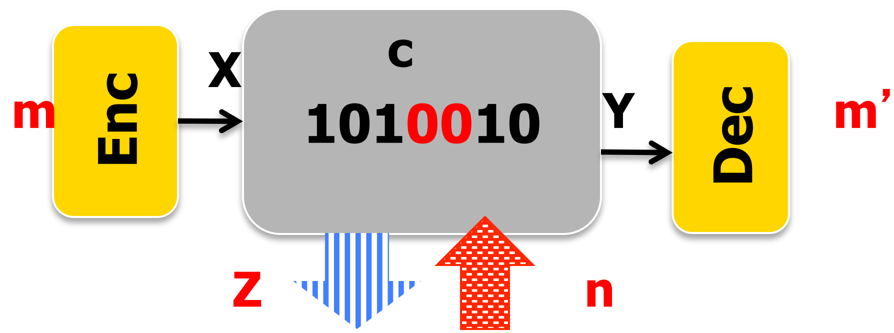
$$\tau(SMT) \geq \frac{1}{1 - 2\rho + \delta'}$$

$$\delta' = \frac{2H(\delta)}{N \log |\Sigma|} + 2\delta$$

Relation with other primitives:

Robust Secret Sharing





$\text{Share}(m,r)=(s_1,s_2\cdots s_L)$

$\text{Reconst}(s_1,s_2\cdots s_t)=m$

$\text{Reconst}(s'_1,s'_2\cdots s'_L)=m'$

$SD(View_A(m_1,r);View_A(m_1,r))=0$

$\Pr(m'\notin\{m,\perp\})\le\delta$

AWTP → Robust SS

- N=2t+1

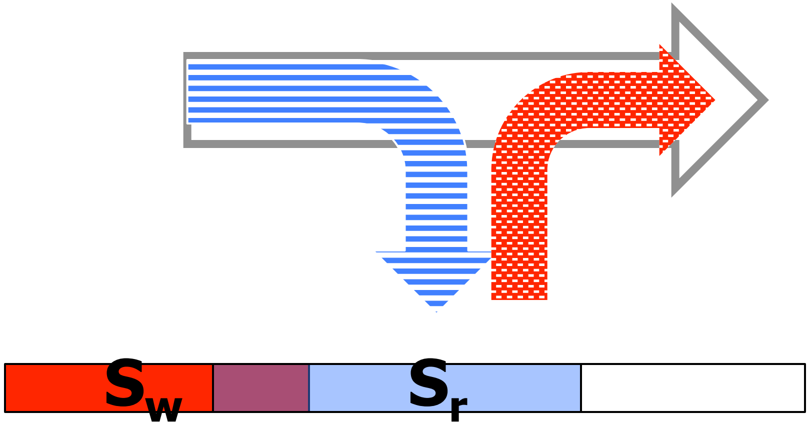
- A more general model of adversary

AWTPenc, AWTPdec → (RSSenc, RSSdec)

Limited View Adversary
Reliability Only

- Theorem

$$C \leq 1 - \rho_w$$



- Comparison: List decodable codes

Limited View Adversary Code

- Building blocks
  1. Message Authentication Codes
  2. AWTP Code
  3. FRS code with subspace evasive set

- Encoding:

$$c_{AWTP} = AWTPenc(r) \qquad c_{FRS} = FRSenc(m, t = MAC(m, r))$$

$$\text{AWTPenc} = \begin{bmatrix} c_{AWTP} \\ c_{FRS} \end{bmatrix}$$

Limited View Adversary Code

- Decoding:
  1. $r = AWTPdec(c_{AWTP})$
  2. $(m_i, t_i) \in L = FRSdec(c_{FRS})$
  3. $t_i = ?\, MAC(m_i, r)$

- Requirement: $\rho_r < 1 - \rho_w$

Concluding remarks

- LV codes with $\rho_r > 1-\rho_w$
- AWTP/LV codes for small alphabet

- Interactive coding
- Key agreement

- AWTP with public discussion