

# LT Codes and Group Codes on the Wiretap channel

Arunkumar Subramanian

Prof. Steven McLaughlin

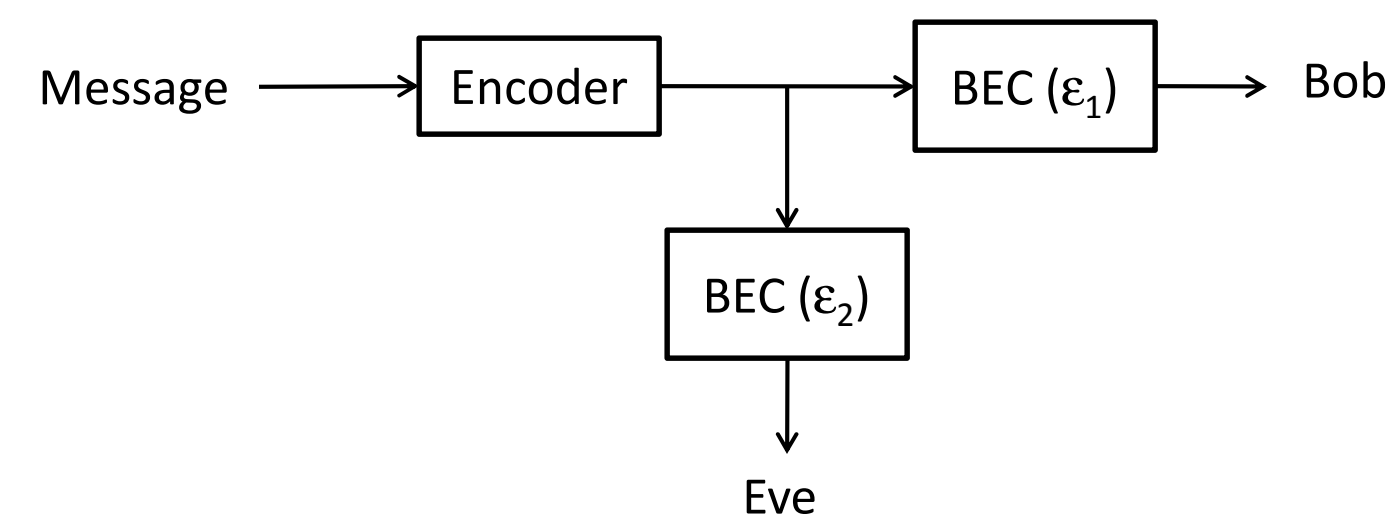
Coding, Communication and Information Theory Group

Georgia Institute of Technology

## Rateless Codes

- Given  $k$  symbols from a field  $F$
- Encoder outputs a sequence of i.i.d. check-symbols from  $F$
- Decoding depends only on the number of check-symbols collected by receiver
- Examples - LT codes, Raptor codes

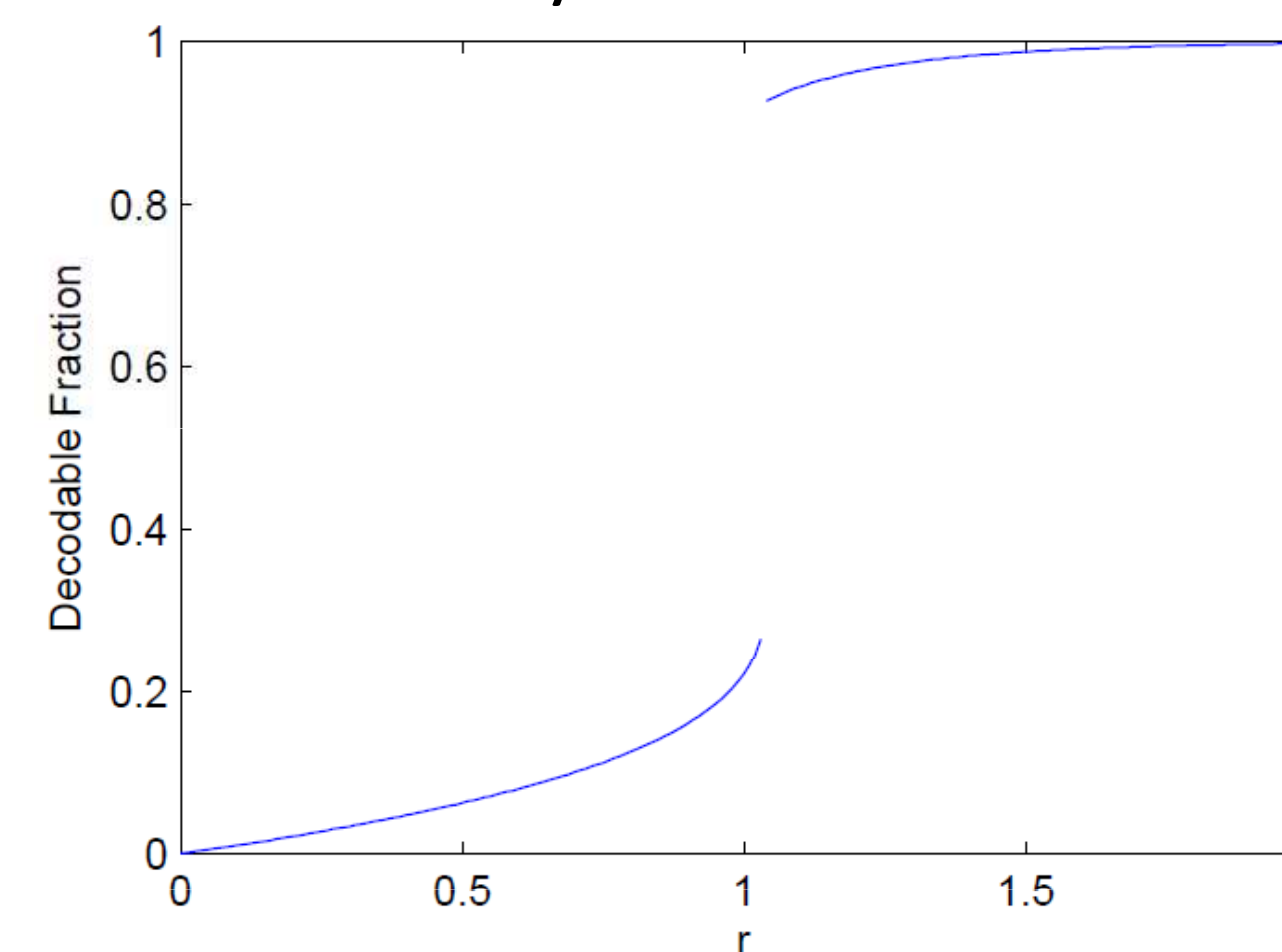
## Channel model and Transmission Scheme



- Truncate LT sequence by  $\text{Poisson}(rk)$
- Bob and Eve receive  $\text{Poisson}((1-\epsilon_i)rk)$  check symbols
- Decodable fraction of message symbols ( $k_1/k$ ) is tractable for Poisson truncation

## Thresholding Property

- Convergence limit,  $z^*$ , need not vary continuously with  $r$



## DLP/LDP of Group Codes

- Given a  $\mu$ , DLP determines the maximum number of codewords that will fit an erasure pattern
- $n - \mu - \text{DLP}(n-\mu)$  gives the wire-tapper's equivocation
- DLP/LDP analysis can be used to find good codes for a particular case of type II wire-tap channel

## Encoding for LT Codes

- Given a message block size  $k$ , and a degree distribution polynomial  $\rho(t)$
- For each  $n \in N$ , encode a check symbol by the following:
  1. Choose a random degree  $d$  using the distribution  $\rho(t)$
  2. Choose  $d$  random message symbols out of the given  $k$
  3. Sum of the chosen symbols gives the check symbol

## Decoding Fraction Convergence

- Define  $z^*$  as
$$z^* = \inf\{t \in [0, 1) : rk\rho'(t) + \log(1-t) < 0\} \wedge 1$$
- If  $rk\rho'(t) + \log(1-t)$  has no zeroes in  $[0, z^*)$ , then
$$\frac{k_1}{k} \rightarrow z^*$$
in probability as  $k \rightarrow \infty$

## Summary

- Our transmission scheme with LT codes has a thresholding property if we choose the degree distribution properly
- A wire-tapper with a slightly worse channel and only a sub-optimal receiver can decode far too less message symbols compared to the legitimate receiver who only has a slightly better channel
- The above is a weaker security criterion – we should use an inner code to completely secure it

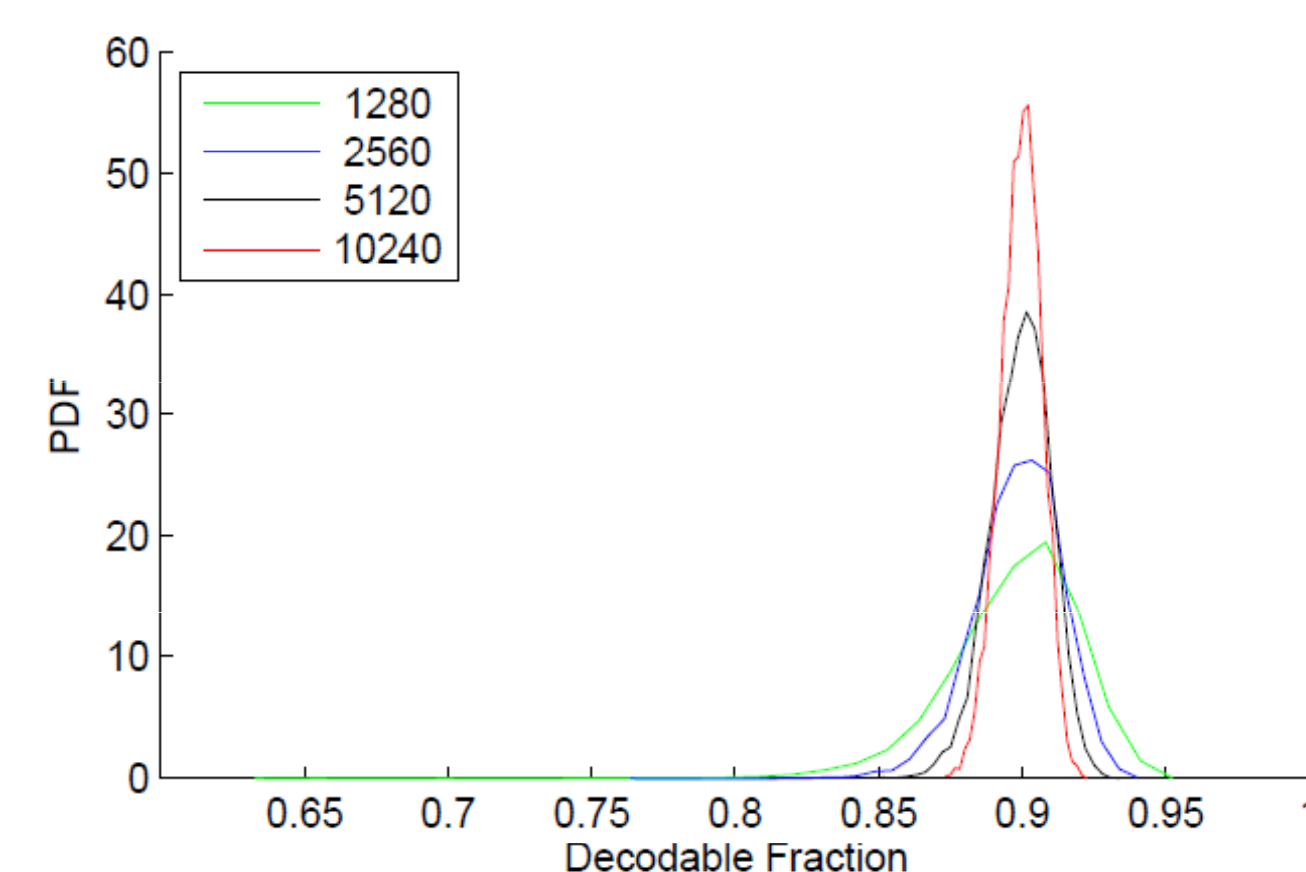
## References

- [1] M. Luby, "LT-codes," in *Proceedings of FOCS*, 2002, pp. 271-280.
- [2] R. Darling and J. Norris, "Structure of large random hypergraphs," *Annals of Applied Probability*, vol. 15, no. 1A, pp. 125–152, 2005.
- [3] R. Darling, D. Levin and J. Norris, "Continuous and Discontinuous Phase transitions in Hypergraph Processes," *Random Struct. Algorithms*, vol. 24, no. 4, pp. 397 – 419, 2004.
- [4] E. Maneva and A. Shokrollahi, "New model for rigorous analysis of LT codes," in *ISIT*, 2006.

## Decoding for LT Codes

- Decoding is done on an evolving graph by eliminating degree one check nodes
- Number of message symbols decoded is dependent on the of number of check symbols collected
- The algorithm is sub-optimal with average complexity  $O(k \log k)$
- The optimal algorithm based on equation solving has complexity  $\geq O(k^2)$

## Convergence in Simulation



## Group Codes on Wiretap II

- Eavesdropper can tap at most  $\mu$  symbols out of  $N$  transmitted symbols
- Main channel is perfect
- Ozarow-Wyner coset coding can achieve perfect secrecy under some conditions
- Given a  $(n, n-k)$  group code  $C$ , we can determine the maximum allowable  $\mu$

## References (contd.)

- [5] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *AT&T Bell Lab. Tech. J.*, vol. 63, pp. 2135–2157, Dec. 1984.
- [6] D. Forney, "Dimension/Length Profiles and Trellis Complexity of Linear Block Codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 6, Nov. 1994.
- [7] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1412 – 1418, Sept. 1991.