Joint Cryptography and Data Compression

João Almeida

Joint work with João Barros

Instituto de Telecomunicações
Faculdade de Engenharia da Universidade do Porto, Portugal
jpa@fe.up.pt

Outline

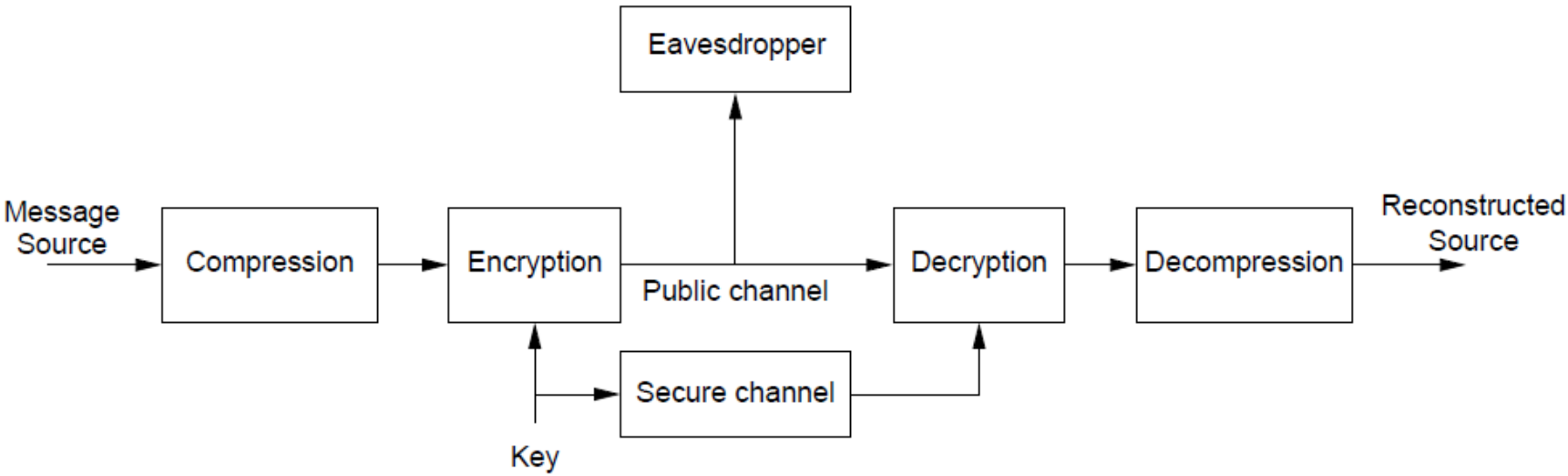
Security - is it worth it?

- Well understood problem with many alternative solutions;
  - Almost all of them are modular;
- Lots of constraints
  - Hardware;
  - Time;
  - Data;
- As lightweight as possible:
  - Try to remove the extra module (go for channel coding, source coding, network coding, ...);

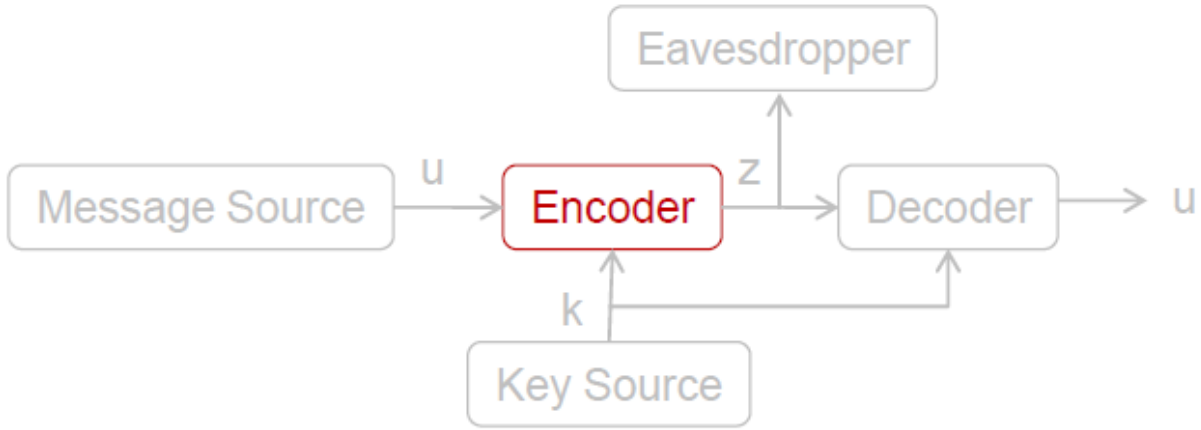
Outline

instituto de telecomunicações

Modular security



Combining compression and encryption



- How can we design such encoder?
  - Explore knowledge given by the source and properties of source encoding algorithms;
  - Use this knowledge to compute cryptograms and key-streams;
  - Analysis-by-synthesis principle;

instituto de telecomunicações

Prospects in variable length codes

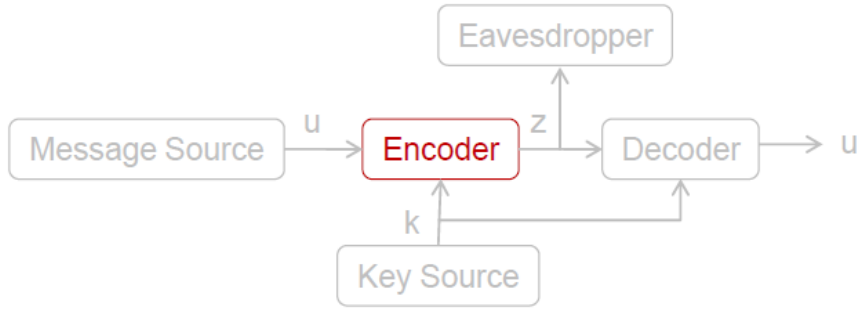
- Catastrophic error propagation:
  - C = {A: 100, B: 0, C: 111, D: 101, E: 110};
  - BBCBECDBBB $\rightarrow$ 0011101101111101000 $\rightarrow$ DBDDCBAB;
  - Symbol error rate depends on the codebook;
- Some effort to analyze error propagation and prevent it (reversible codes, synchronizing codewords, ...);

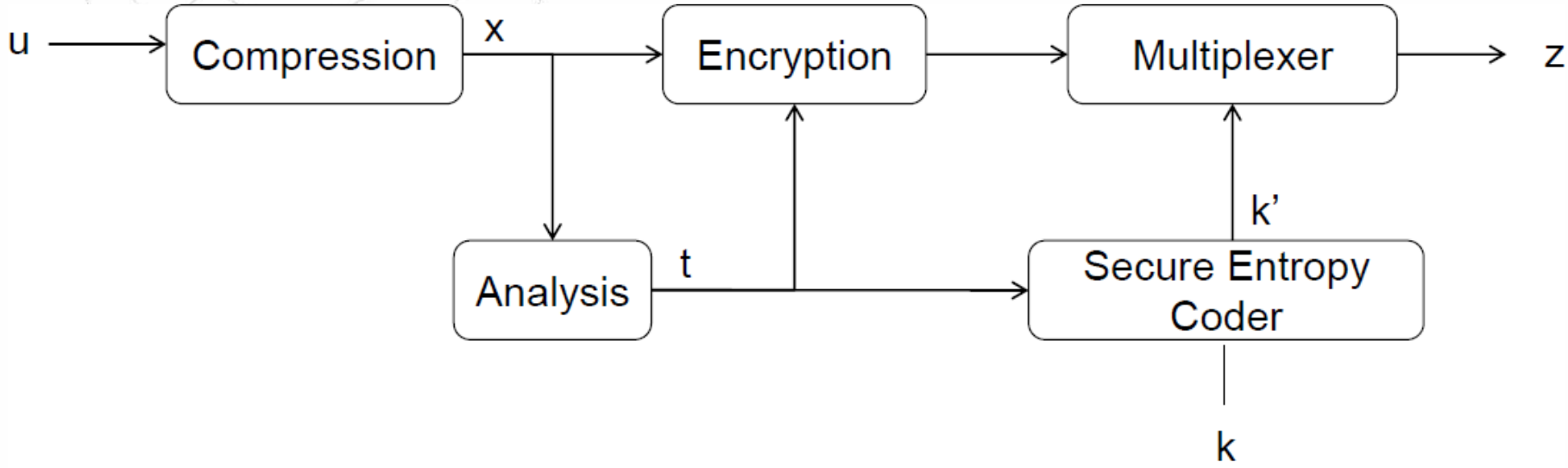
Prospects in variable length codes

- Catastrophic error propagation:
  - C = {A: 100, B: 0, C: 111, D: 101, E: 110};
  - BBCBECDBBB $\rightarrow$ 0011101101111101000 $\rightarrow$ DBDDCBAB;
  - Symbol error rate depends on the codebook;
- Some effort to analyze error propagation and prevent it (reversible codes, synchronizing codewords, ...);
- ... catastrophic error propagation can be useful;
  - Error patterns $\leftrightarrow$ key-streams;
  - Carefully induce errors...
  - Unfortunately the decoder must also know where these errors have been introduced;
  - Share it or send it?

instituto de telecomunicações

Detailed encoder

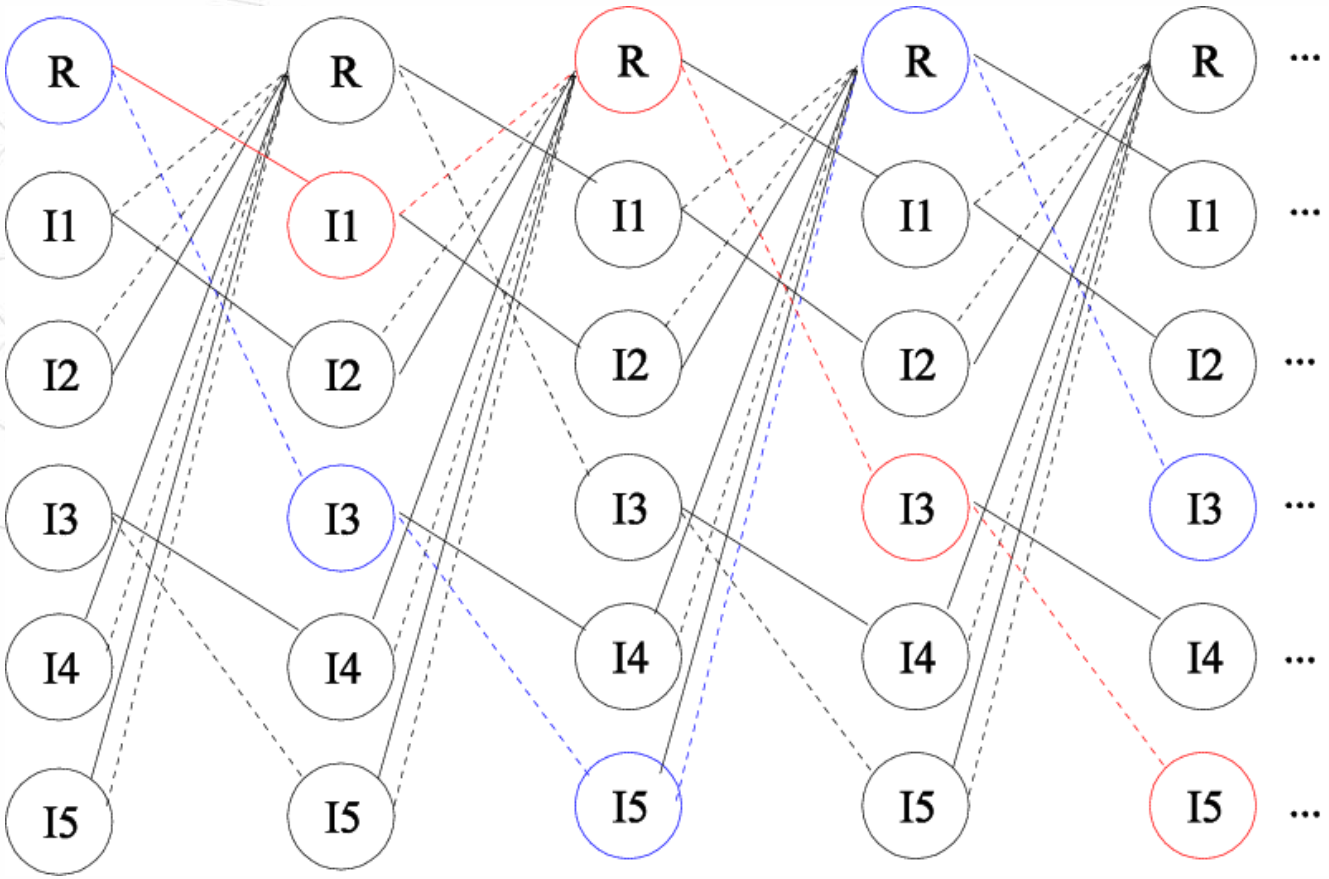




instituto de telecomunicações

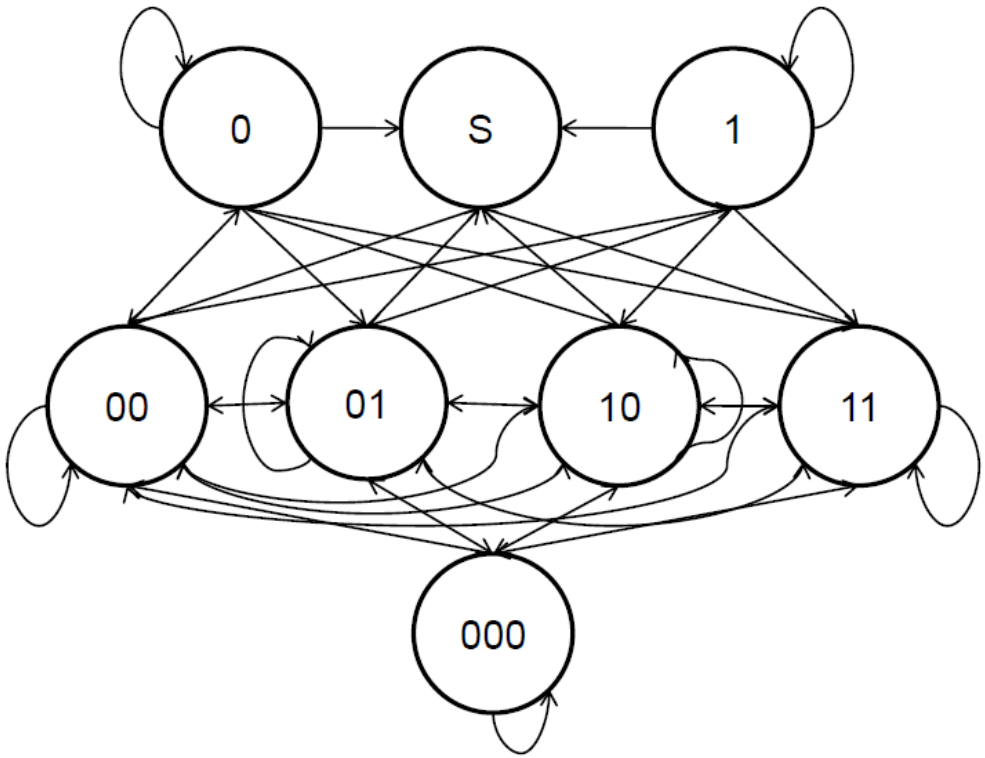
Outline

Algorithm I



Algorithm II

s	x		t	
I	-		-	
0	0000	C	0010	Y
0	010	R	000	Y
1	001	Y	010	Y
1	011	P	000	O
0	100	T	000	H
1	101	O	000	R
1	111	G	000	G
0	010	R	000	O
1	0001	A	0000	C
1	011	P	000	O
0	110	H	000	G
S	001	Y	000	A

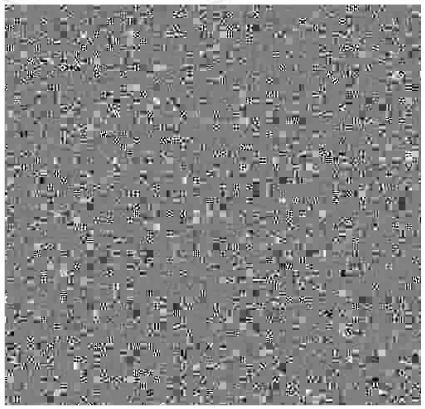


instituto de telecomunicações

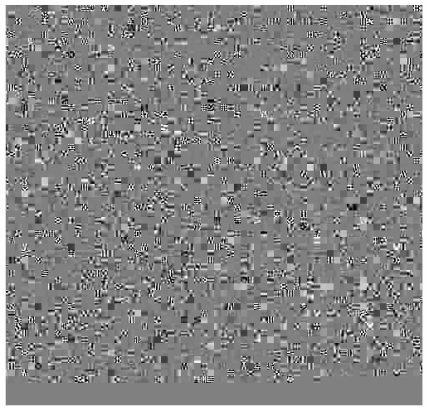
Example: baseline JPEG

(a) Original image

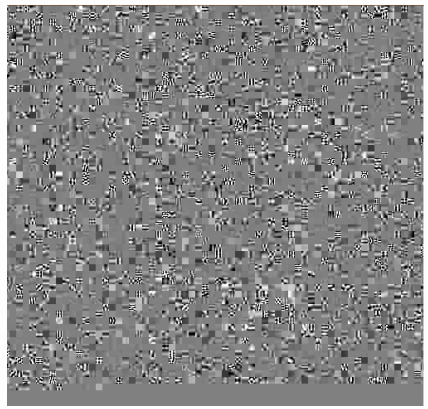
(b) Recovered image



(c) Algorithm I (R = 0.17)



(d) Algorithm IIa (R = 0.49)



(e) Algorithm IIb (R = 0.27)

instituto de telecomunicações

Wrapping up

- Low complexity:
  - Algorithm I: $\mathcal{O}(k \cdot p)$, where k is the length of the input bit-stream and p the number of states in the trellis;
  - Algorithm II: $\mathcal{O}(n)$, where n is the size of the source message;
- Inducing loss of sync:
  - Leads to compressible key-streams;
- Codeword size diversity might become an issue:
  - Use super-symbols;

instituto de telecomunicações

Outline

Take home messages!

- Computational constraints ask for lightweight cryptography:
  - Coding schemes are good options;
- Modular approaches are insensitive to underlying communication blocks:
  - Jointly design compression and encryption stages;
- Leverage from source knowledge and encoder properties:
  - Analysis-by-synthesis encoding;
- Variable length codes:
  - Use error-patterns as key-streams (catastrophic error propagation);
  - Induce loss of synchronization;
- Further developments:
  - Secure entropy encoders;
  - Algorithms for other source encoders;

instituto de telecomunicações

Q & A

Thank you for the attention!
Questions?

instituto de telecomunicações