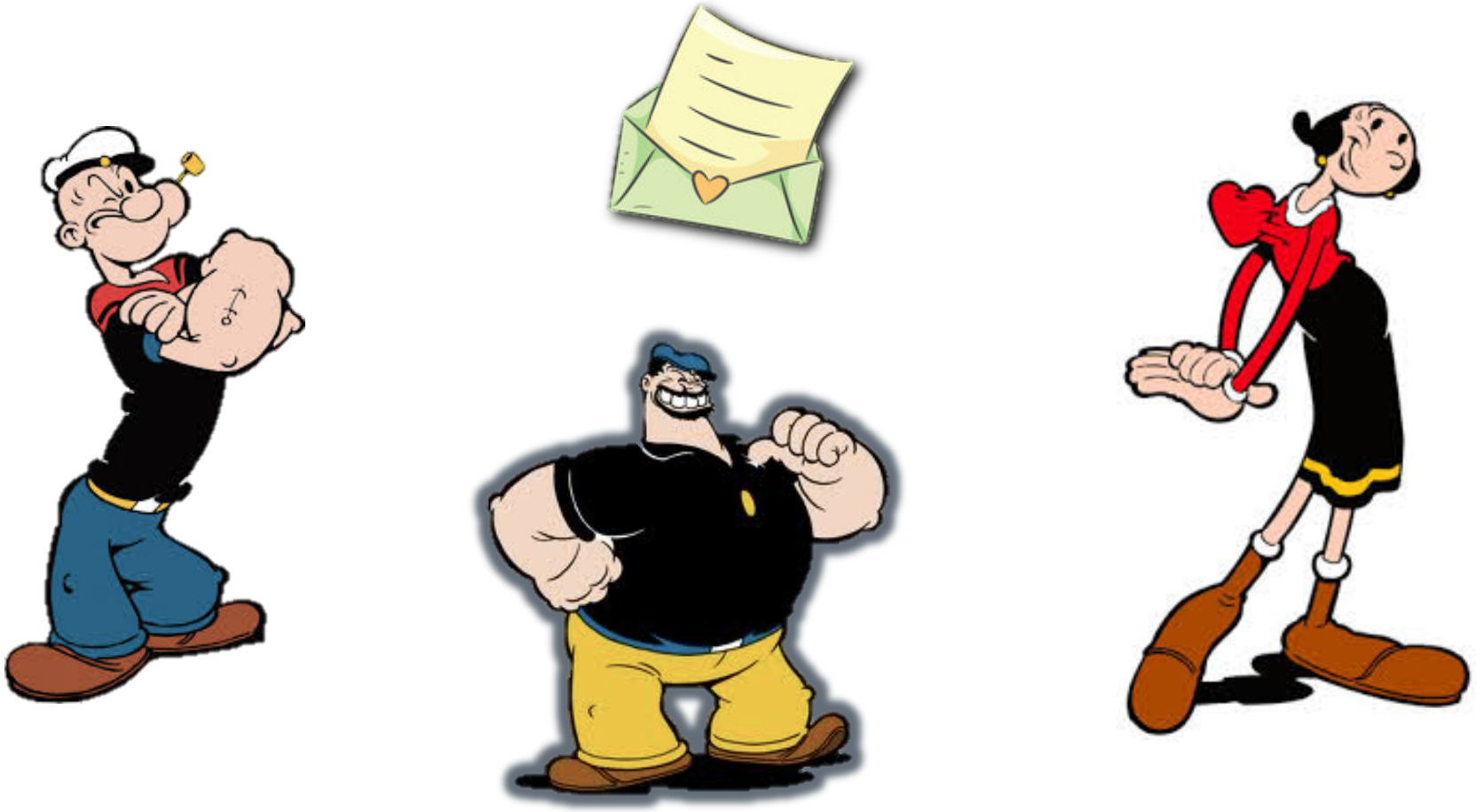
“ Information authentication for linear-coding-based communication networks: Homomorphic Message Authentication Codes ”

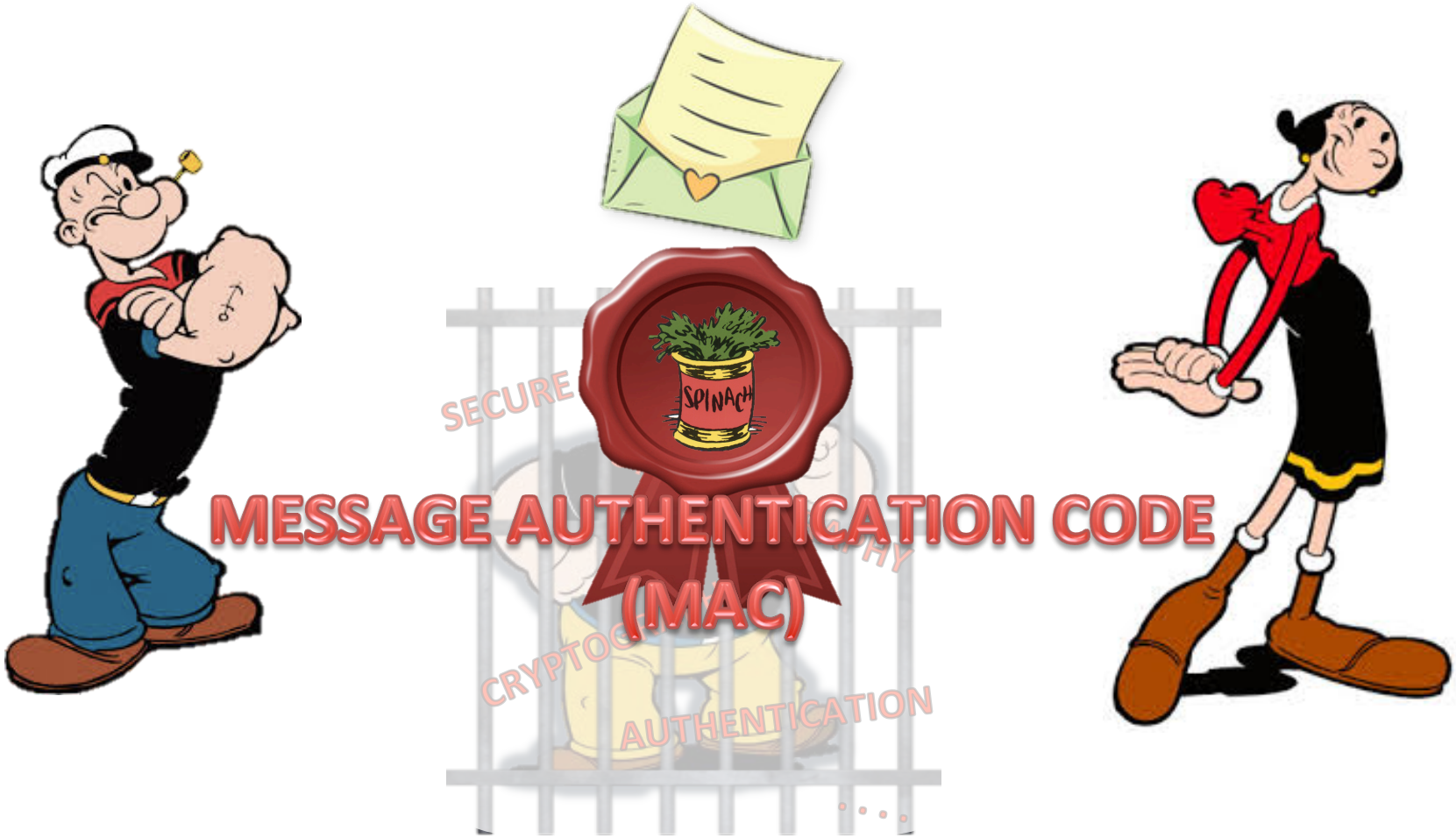
Why do we need information authentication?

Why do we need information authentication?



Why do we need information authentication?

Why do we need information authentication?

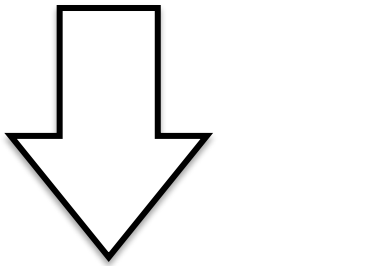


MACs (intuitive idea)

MACs (intuitive idea)

MACs (intuitive idea)

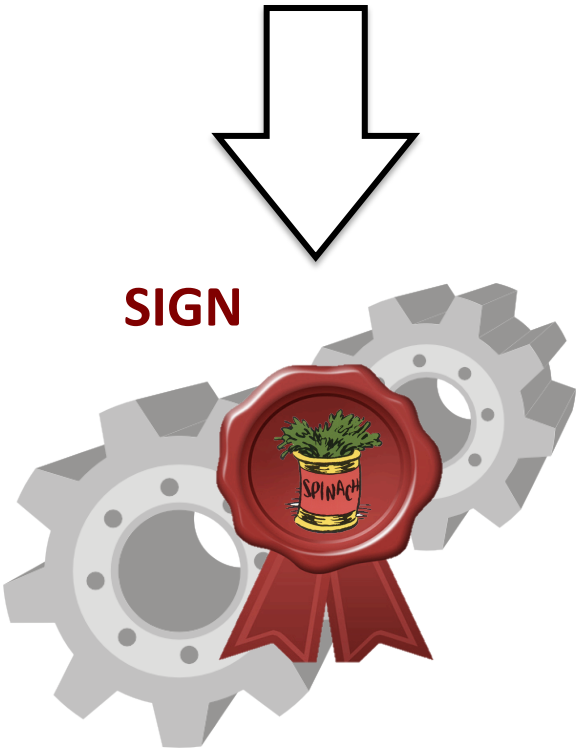
message



SIGN

MACs (intuitive idea)

message



tag

MACs (intuitive idea)

message

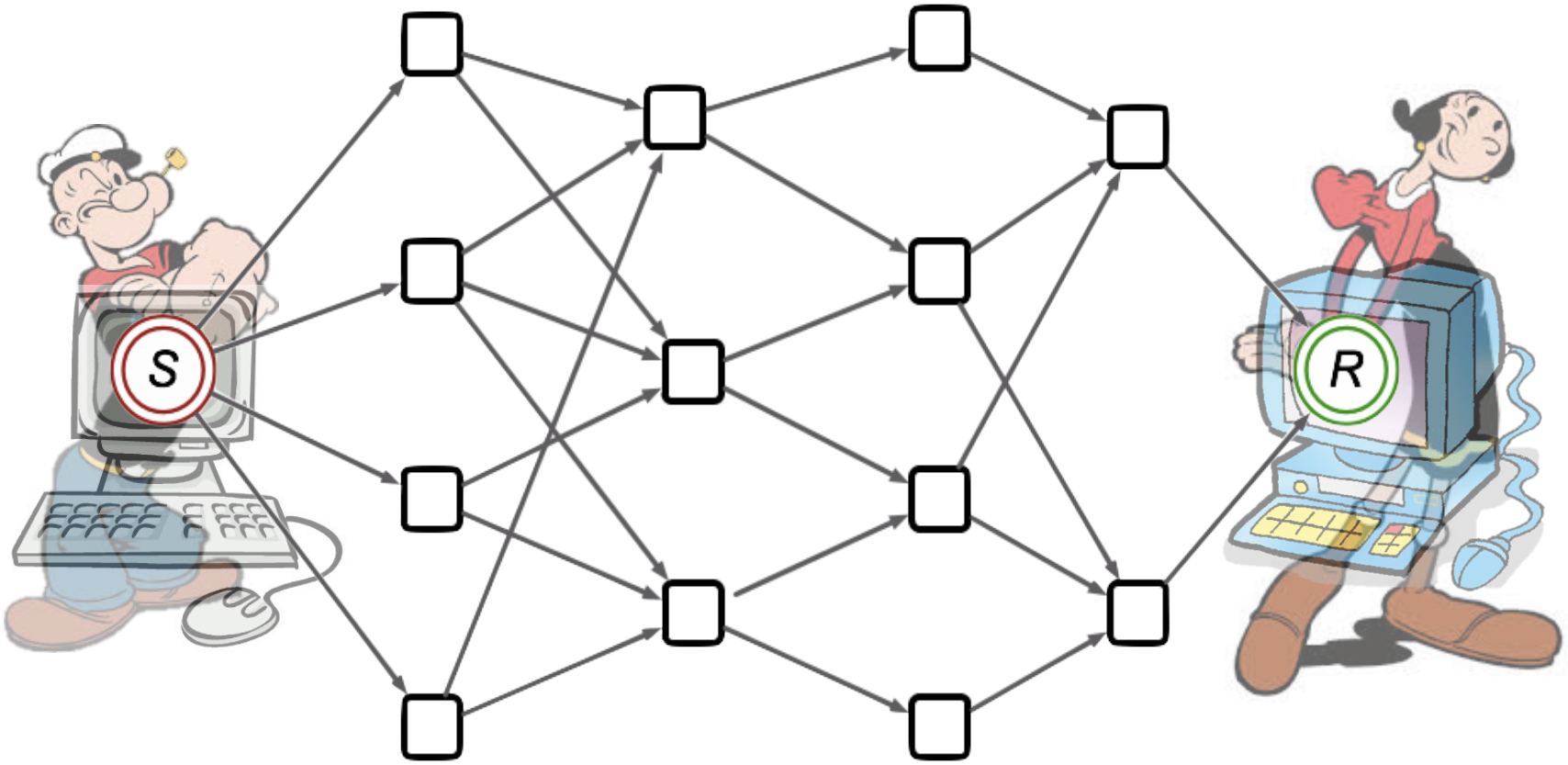
tag

MACs (intuitive idea)

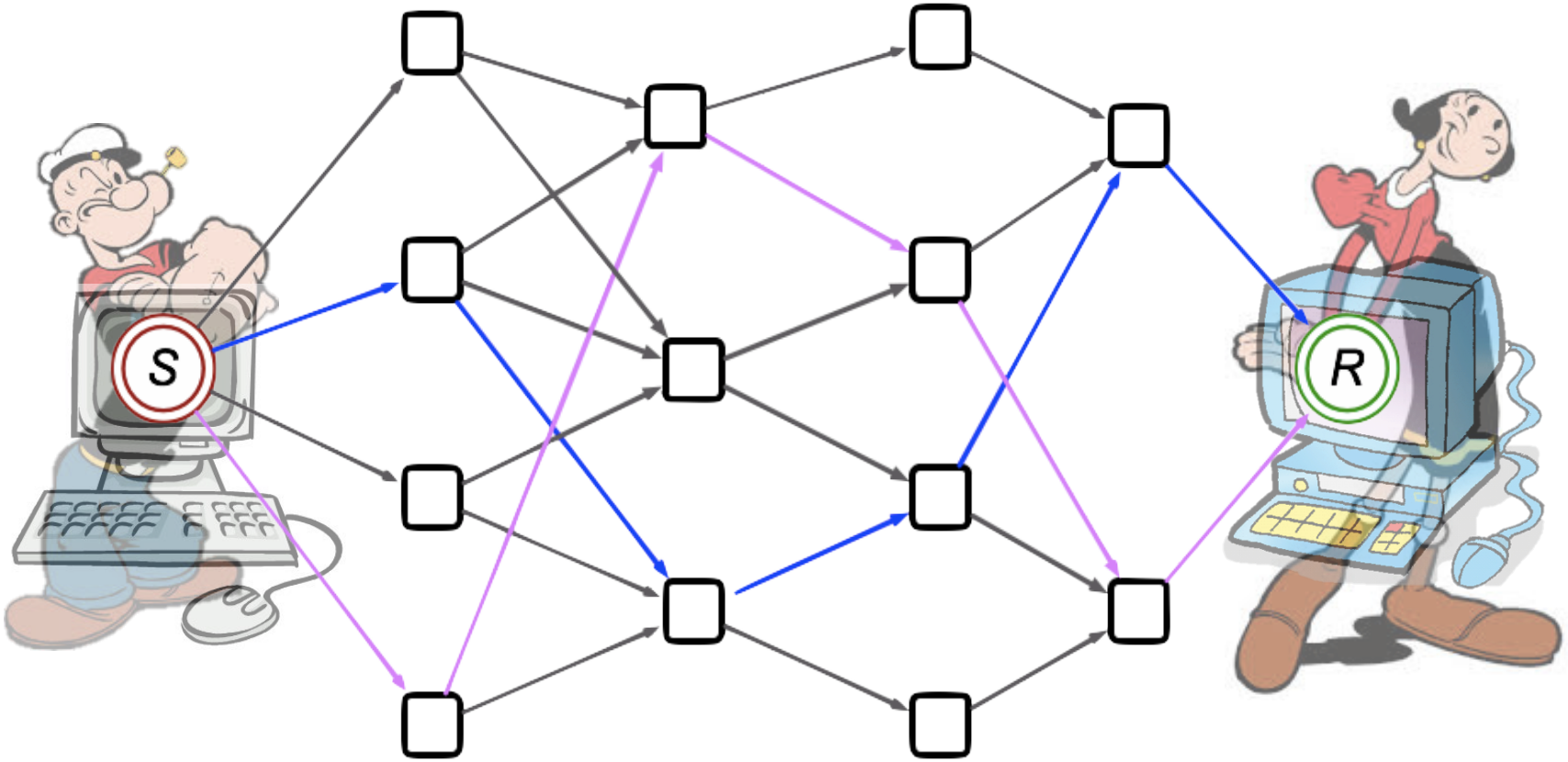
message

tag

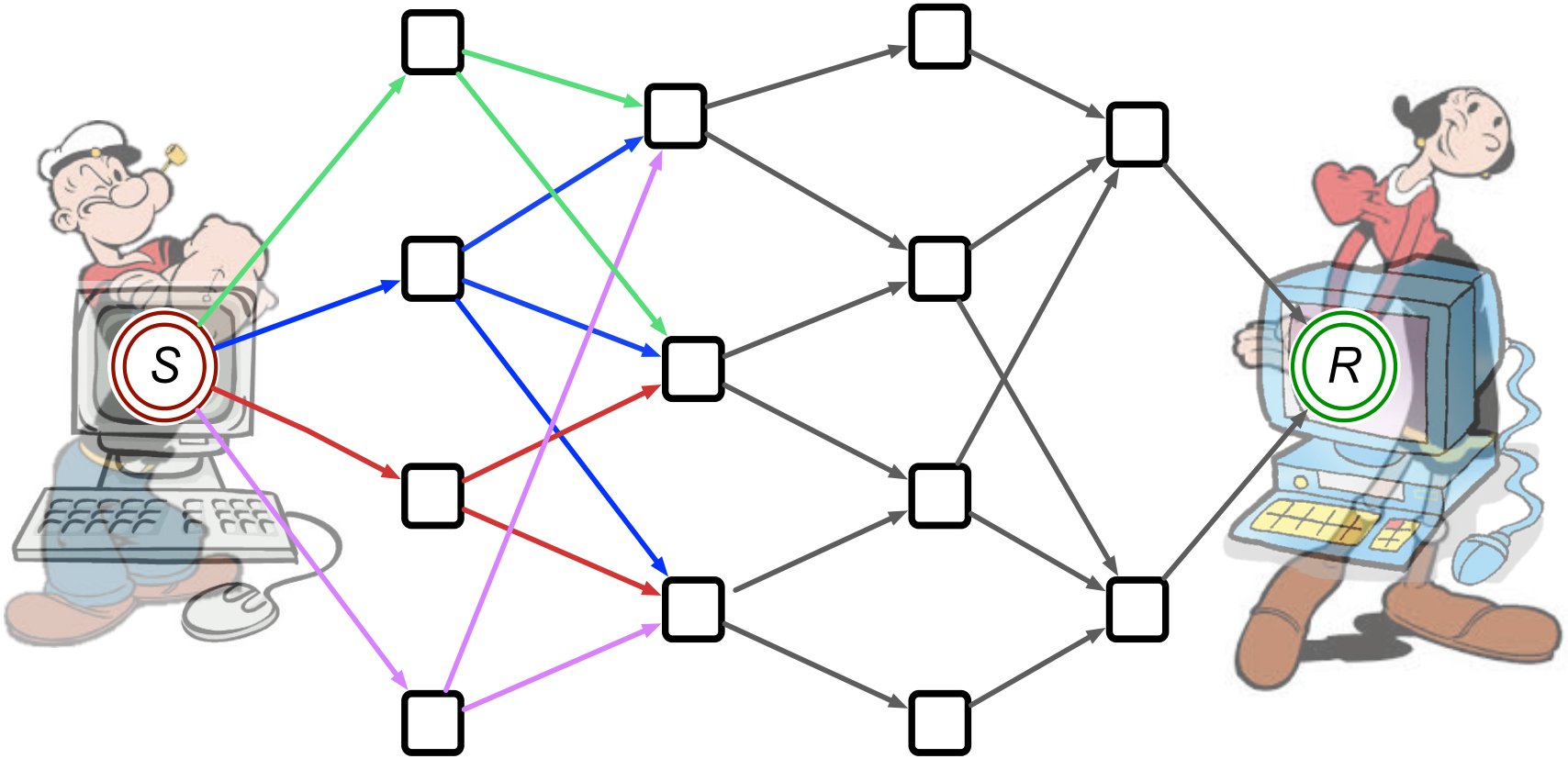
Linear Network Coding



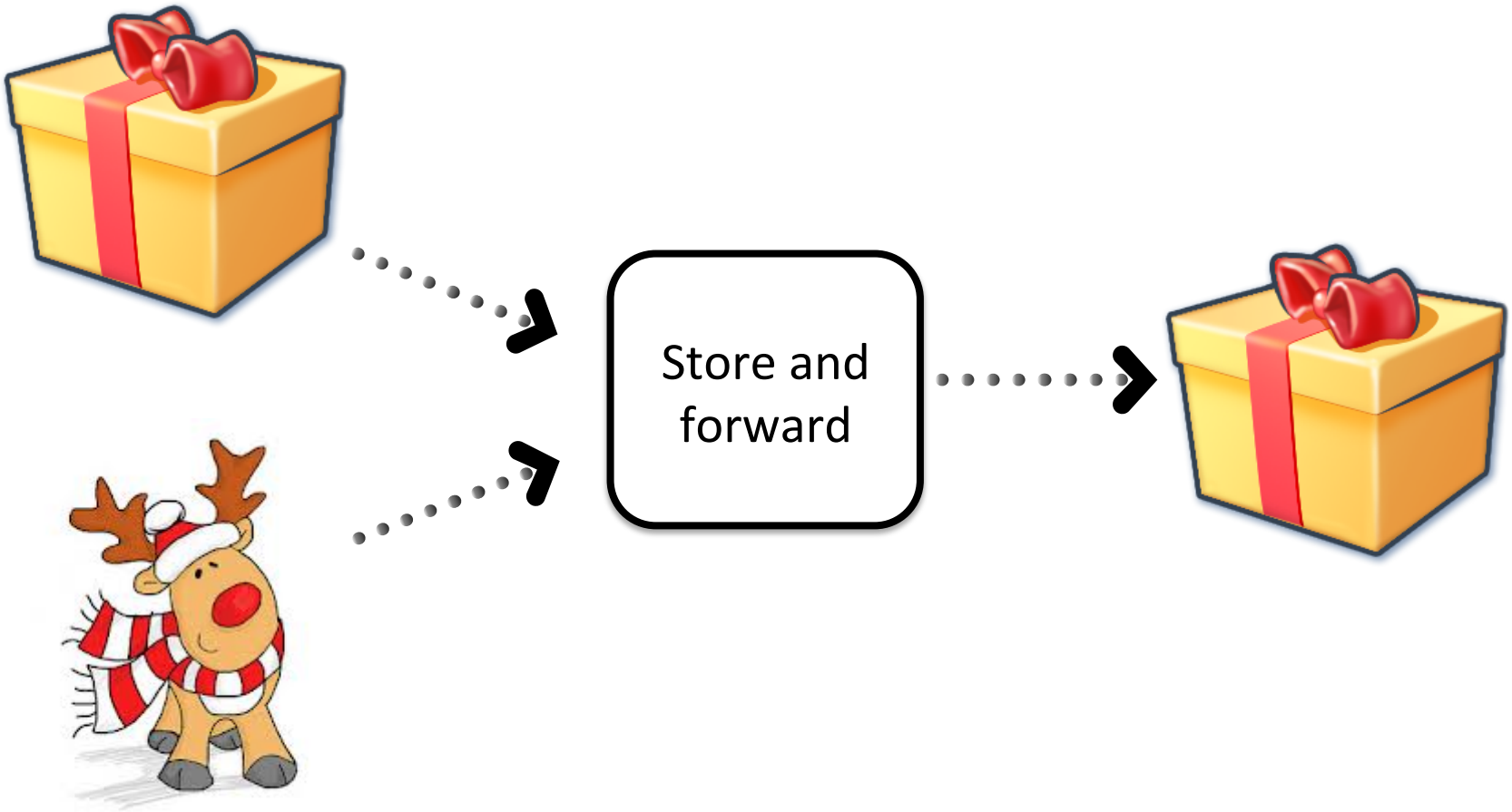
Linear Network Coding



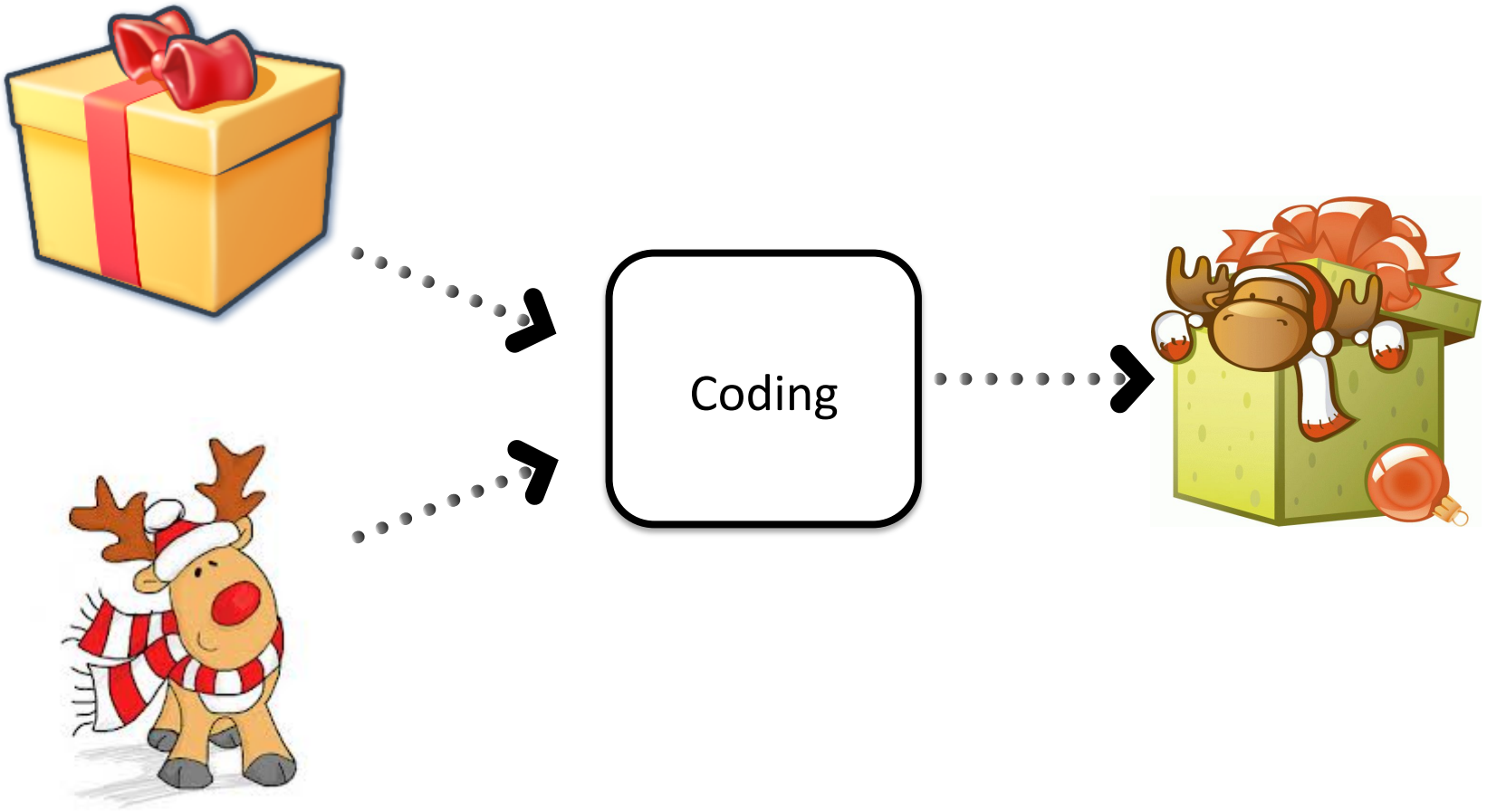
Linear Network Coding



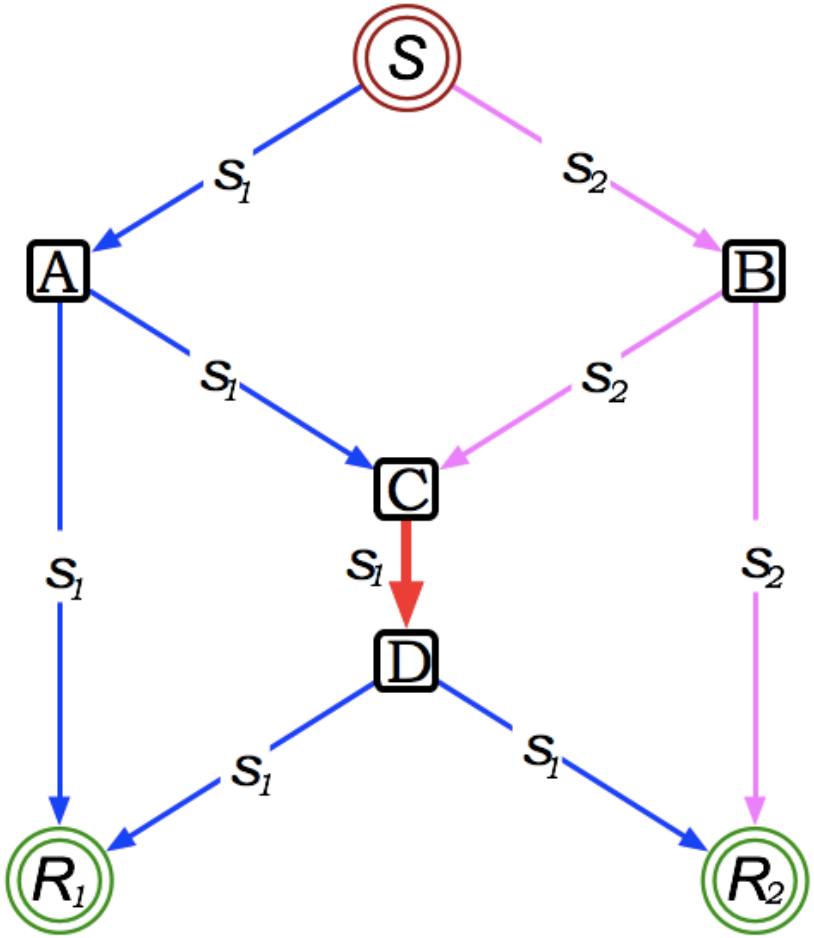
Linear Network Coding



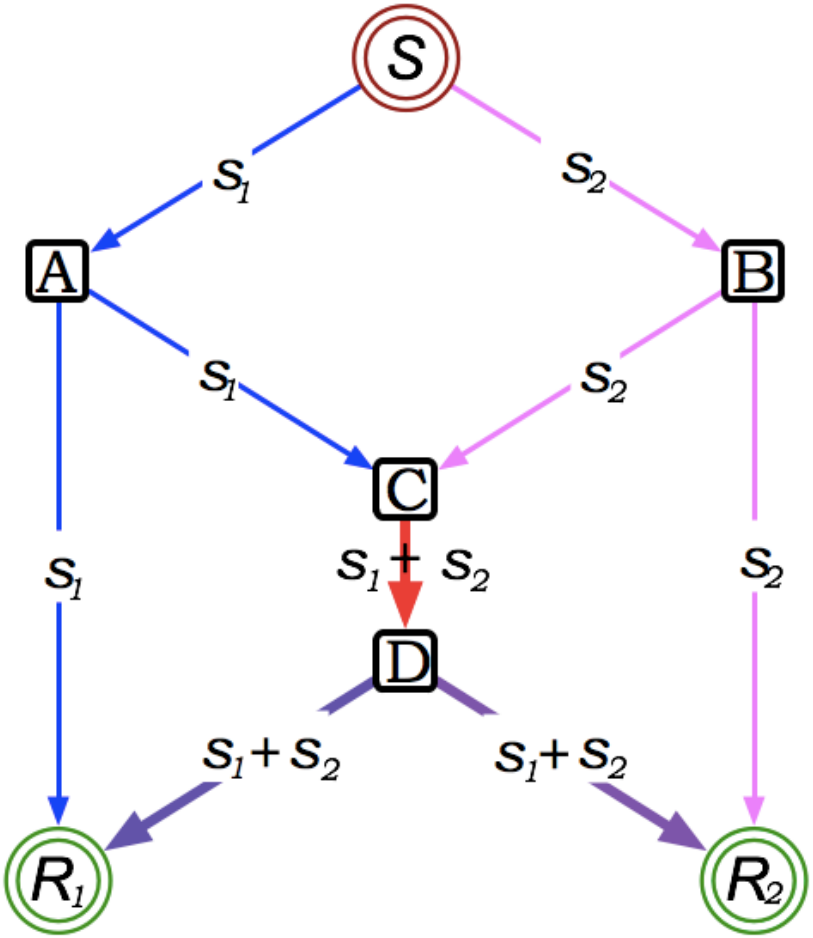
Linear Network Coding



Linear Network Coding



Store & forward network
(edges of capacity 1)



Linear-coding network
(edges of capacity 1)

Where is this useful?

Digital file distribution and peer-to-peer file sharing,

multisource multicasting communications in dynamic networks,

networks with large numbers of nodes,

distributed data storage.

Contact info:

Elena Pagnin (elenap@chalmers.se)

Katerina Mitrokotsa (aikmtr@chalmers.se)