On the Shannon Cipher System with a Capacity–Limited Key Distribution Channel

Neri Merhav

Department of Electrical Engineering

Technion—Israel Institute of Technology

Haifa 32000, Israel

The 44th Annual Allerton Conference on C^3:

Monticello, IL, September 28, 2006

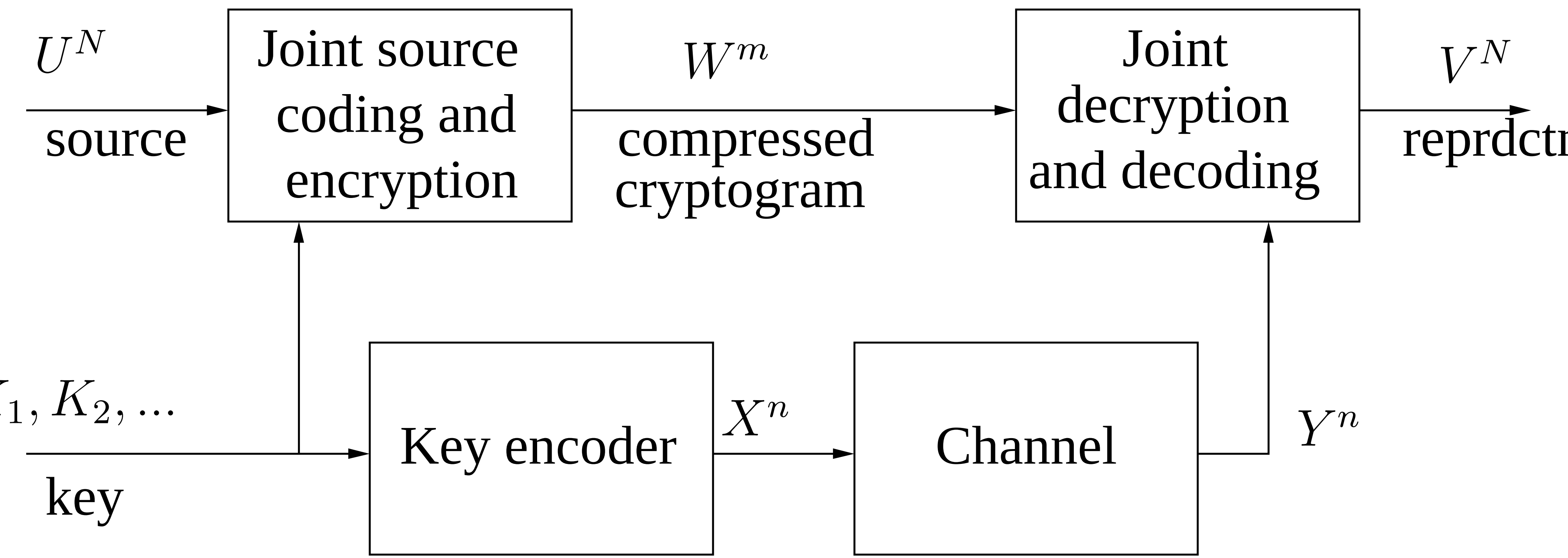
General

In the classical Shannon–theoretic setting of cipher systems, a few assumptions are commonly made:

- The reconstruction of the plaintext should be error–free.
- The encryption and decryption are carried out using the same key.
- The secure channel through which the key is delivered, is clean.

Yamamoto (1997) relaxed the first assumption.

Let us examine what happens also in the abence of the two other assumptions.



U^N
source
Joint source coding and encryption
W^m
compressed cryptogram
Joint decryption and decoding
V^N
reprdctn
$K_1, K_2, ...$
key
Key encoder
X^n
Channel
Y^n

Problem Description

Given a:

- source $P(U^N) = P(U_1)P(U_2)\ldots P(U_N)$,
- a distortion measure $d : \mathcal{U} \times \mathcal{V} \to \mathbb{R}^+$,
- an unlimited reservoir of key bits $\boldsymbol{K} = (K_1, K_2, \ldots)$, and
- a DMC $P(Y^n|X^n) = P(Y_1|X_1)P(Y_2|X_2)\ldots P(Y_n|X_n)$,

Problem Description (Cont'd)

we seek an encoder

$$W^m = f(U^N, \boldsymbol{K}); \qquad X^n = g(\boldsymbol{K})$$

and a decoder

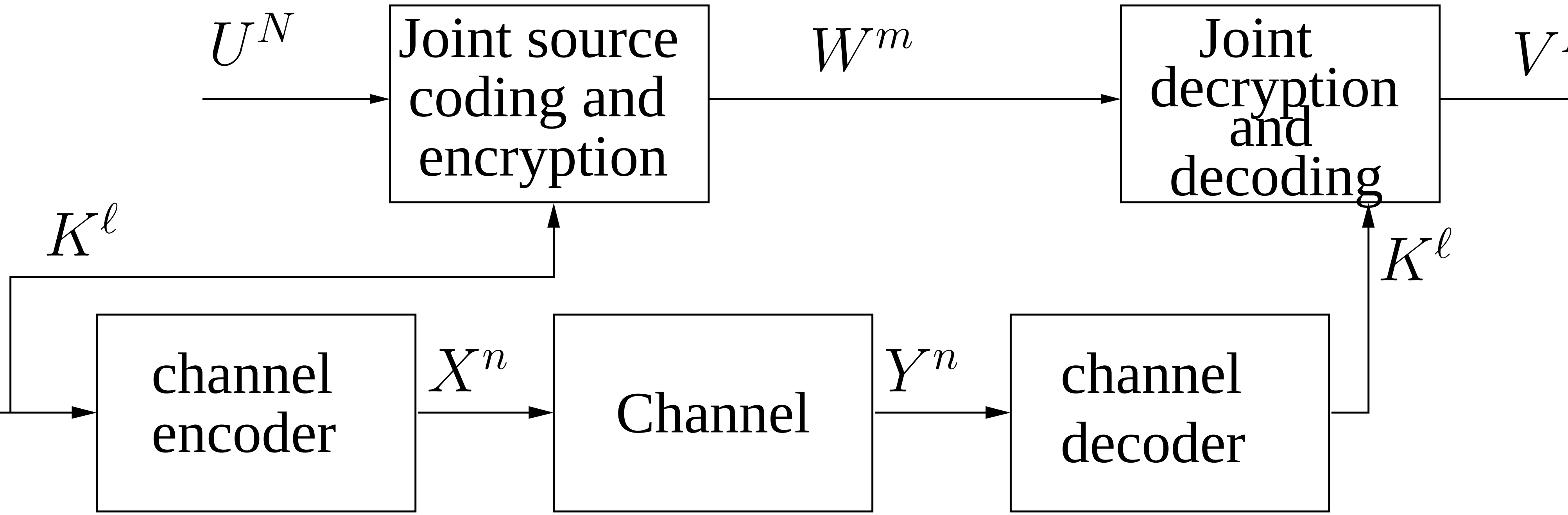
$$V^N = h(W^m, Y^n)$$

such that:

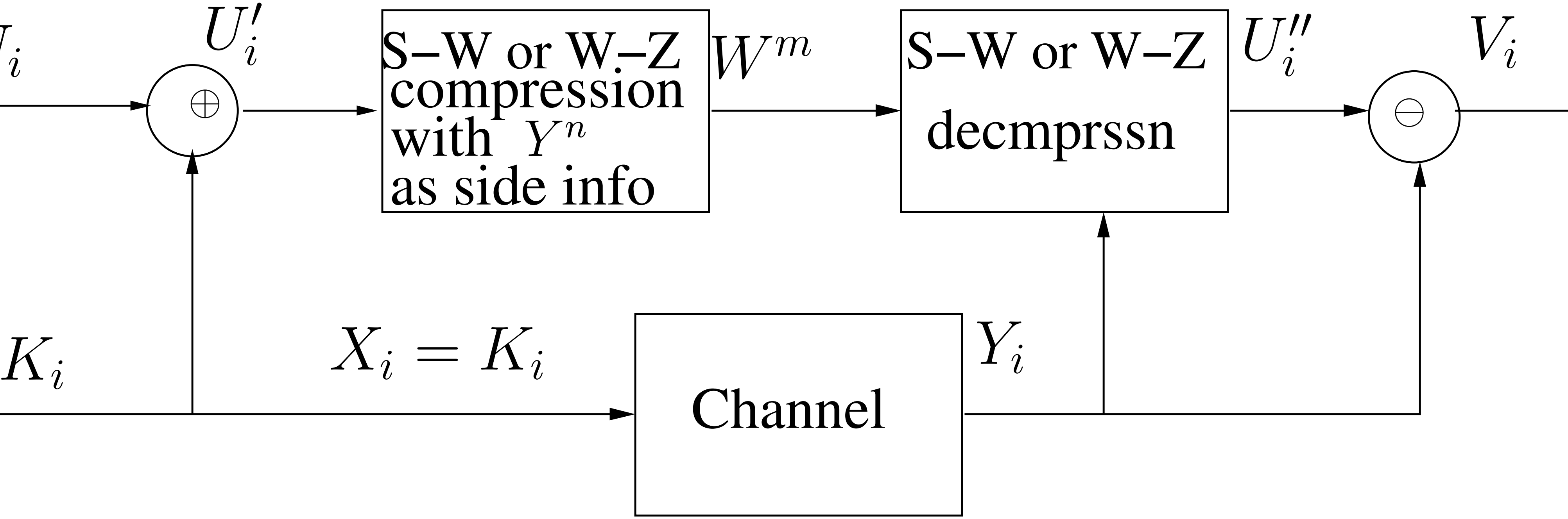
$$\sum_{i=1}^{N} \boldsymbol{E}\{d(U_i, V_i) \leq ND, \quad \mu = \frac{m}{N} \leq R_c, \text{ and } H(U^N|W^m) \geq Nh.$$

What is the achievable region of $\{(D, R_c, h)\}$ and how can we achieve it?

Solution 1: Separate channel coding for the key

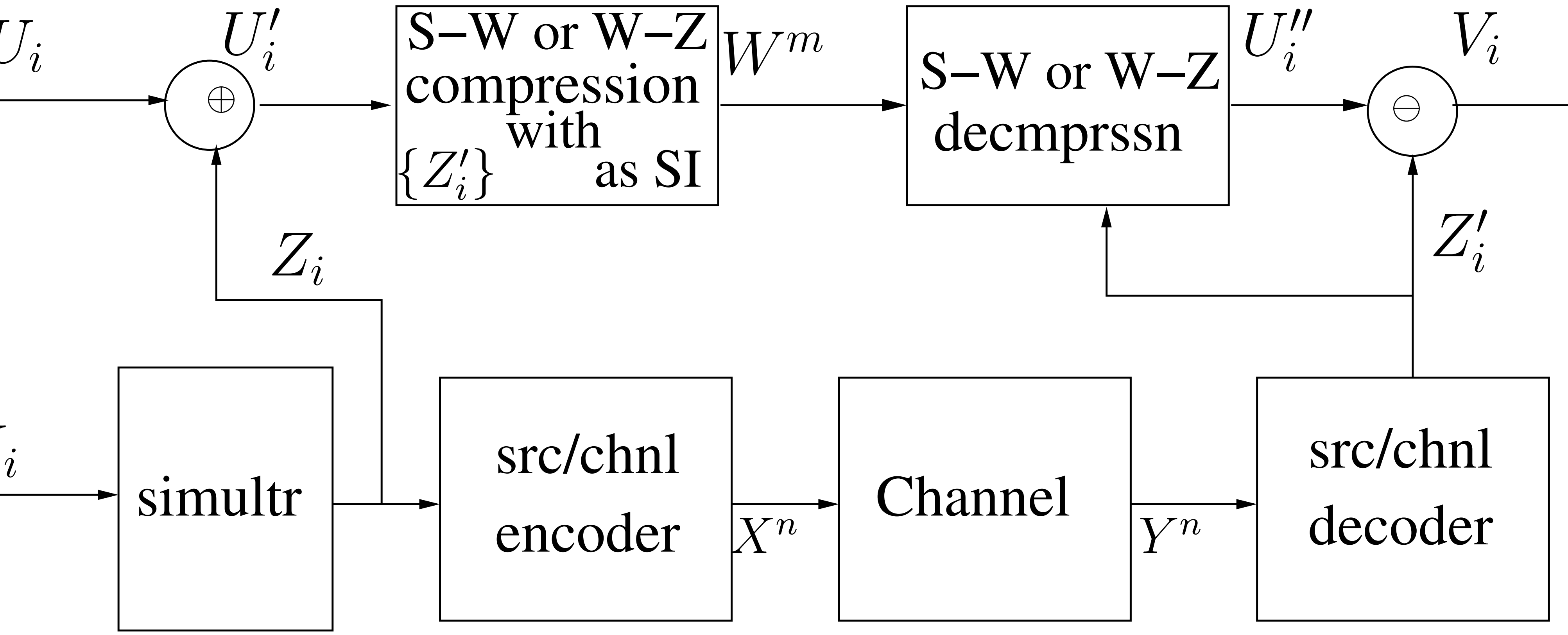


Solution 2: Encrypt and Compress with SI

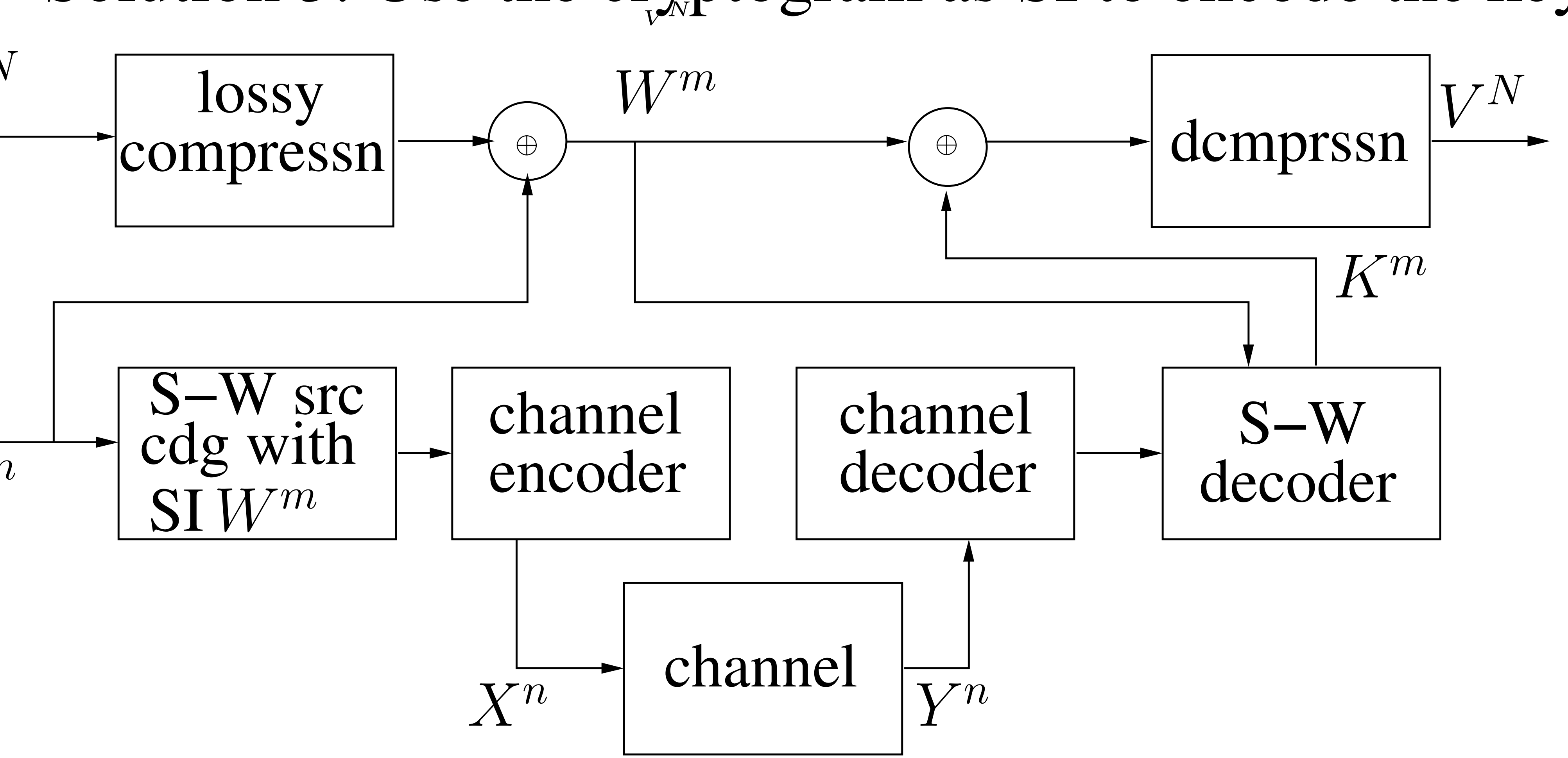


ohnson et. al. (2004)

Solution 2': Encrypt and Compress with SI



Solution 3: Use the cryptogram as SI to encode the key



Informal Description of the Main Result

We show that no solution is better than the first one, namely:

- Transmit $\min\{nC, NR(D)\}$ key bits reliably by channel coding.
- Compress U^N to $NR(D)$ bits.
- Use the key bits to encrypt (one–time pad) the compressed bit–stream.
- At the receiver: decode the key, decrypt the bit–stream, and decompress.

Informal Description of Main Result (Cont'd)

This result is in the spirit of the classical source–channel separation theorem:

- Complete decoupling between source coding (of U^N) and channel coding (of the key).
- Best strategy of controlling the distortion is by rate–distortion coding.
- A necessary and sufficient condition for perfect secrecy is: $R(D) \leq \lambda C$, $\lambda = n/N$.

Coding Theorem

A triple (D, R_c, h) is achievable iff the following two conditions hold:

- $h \leq h(D) \stackrel{\Delta}{=} H(U) - [R(D) - \lambda C]_+$, and
- $R_c \geq R(D)$.

Comments:

- For a given D: no conflict between minimizing R_c and maximizing h.
- Perfect secrecy – $h = H(U)$ can be achieved iff $R(D) - \lambda C \leq 0$.

Simple Coding in Some Special Cases

Suppose that the compressibility of W^m is not an issue ($R_c = \infty$).

As in ordinary joint source–channel coding, there are situations where simple single–letter codes are optimal as in Gastpar (2003).

For example, let us suppose that:

- U is uniform and $\mathcal{U} = \mathcal{X} = \mathcal{Y} = \mathcal{V}$, whose cardinality is a power of 2,
- $\lambda = 1$, $N = n = 1$.
- d – a difference distortion measure, $d(u, v) = \rho(u \ominus v) = \rho(v \ominus u)$.
- C – achieved by the uniform input distribution, and
- $P(Y|X)$ – is the test channel that achieves the rate–distortion function of the uniform distribution.

Simple Coding in Some Special Cases (Cont'd)

Then, the following simple scheme is optimal:

- Generate a uniform RV X on $\mathcal{X}$ using $\log|\mathcal{X}|$ bits from $\boldsymbol{K}$.
- Encryption: $W = U \oplus X$.
- Send X via the channel as is.
- At the receiver, decrypt: $V = W \ominus Y$.

In this case, we have:

- Equivocation: $H(U|W) = \log|\mathcal{X}|$ which is perfect secrecy.
- Distortion: $\boldsymbol{E}\rho(U \ominus V) = \boldsymbol{E}\rho(X \ominus Y) = D = R_U^{-1}(C)$.

Securing the Reproduction V^N

Suppose that there is an additional security requirement:

$$H(V^N|W^m) \geq Nh'.$$

A restatement of the necessity part of our coding theorem is as follows:

If (D, R_c, h, h') is achievable, then there exist a channel $P(V|U)$ and a source $P(X)$ such that the following inequalities hold at the same time:

- $h \leq H(U) - [I(U;V) - \lambda I(X;Y)]_+, \quad h' \leq \min\{H(V), \lambda H(Y)\}$,
- $R_c \geq I(U;V), \quad D \geq \boldsymbol{E}d(U,V)$.

$H(Y) = I(X;Y) + H(Y|X) =$reliable key–rate via channel$+$randomness generated by the channel.

We don't maximize $I(X;Y)$ and minimize $I(U;V)$ because of $H(V)$ and $H(Y)$.

Thus, there is no full separation in this setting!

Securing the Reproduction V^N (Cont'd)

The achievability of the this region of $\{(D, R_c, h, h')\}$ remains open in general.

However, it is known at least for the case of a deterministic channel

$H(Y|X) = 0$, in which case, we can again maximize

$$C = \max_X I(X;Y) = \max_X H(Y)$$

but still cannot minimize $I(U;V)$.

Securing the Reproduction V^N (Cont'd)

The achievability is based on the fact that given $P(U, V)$, $\exists \approx 2^{NH(V|U)}$ distinct rate–distortion codebooks, each of size $2^{NI(U;V)}$ that produce a jointly typical V^N for every typical input U^N.

The coding scheme works as follows:

- If $H(V) \leq \lambda C$, use $NH(V|U)$ key bits to choose a codebook plus $NI(U; V)$ key bits to encrypt the codeword.
- If $I(U; V) \leq \lambda C \leq H(V)$, use $nC - NI(U; V)$ key bits to choose a codebook plus $NI(U; V)$ key bits to encrypt the codeword.
- If $\lambda C \leq I(U; V)$, use nC key bits to partially encrypt the codeword (of one specified codebook).

Feedback

Suppose that prior to the encryption/compression of U^N, the transmitter receives noiseless feedback of Y^n. This is similar to a deterministic channel $(X^n, Y^n) \to Y^n$.

- It is clear too how to secure V^N to the (maximum) level $h' = \min\{H(V), \lambda H(Y)\}$ (simply use Y^n alone as the common key).
- The security of U^N can be enhanced to the (maximum) level $h = H(U) - [I(U;V) - \lambda H(Y)]_+$.
- Here, $\boldsymbol{K}$ is just used to simulate an input X that maximizes $H(Y)$.

Thus, although feedback does not increase capacity of a DMC, it improves its effectiveness when this channel is harnessed for delivering a key.

Conclusion

- We addressed the problem of joint lossly compression and encryption when the key delivery channel is of limited capacity.
- We characterized the achievable region of D, R_c, and h.
- This characterization suggests a “separation theorem.”
- When the security of the reproduction becomes a factor, separation fails.
- There is a gap between the necessary and sufficient conditions, which vanishes when the channel is deterministic or when there is feedback.