Perfectly Secure Encryption of Individual Sequences

Neri Merhav

Department of Electrical Engineering

Technion—Israel Institute of Technology

Haifa 32000, Israel

ISIT 2012, Cambridge, MA, July 2012.

Background and Motivation

The individual–sequence approach (with FSM's) to IT has been studied in:

- Data compression (Ziv & Lempel '78,...).
- Source/channel simulation (Martín *et al.* '10, Seroussi '06).
- Classification (Ziv & Merhav, '93).
- Prediction (Feder, Merhav & Gutman '92, ...).
- Denoising (Weissman *et al.*, '05,...).
- Channel coding (Lomnitz & Feder '10, Shayevitz & Feder '05).

Information–theoretic security has been studied almost exclusively from the probabilisitic approach.

Background and Motivation (Cont'd)

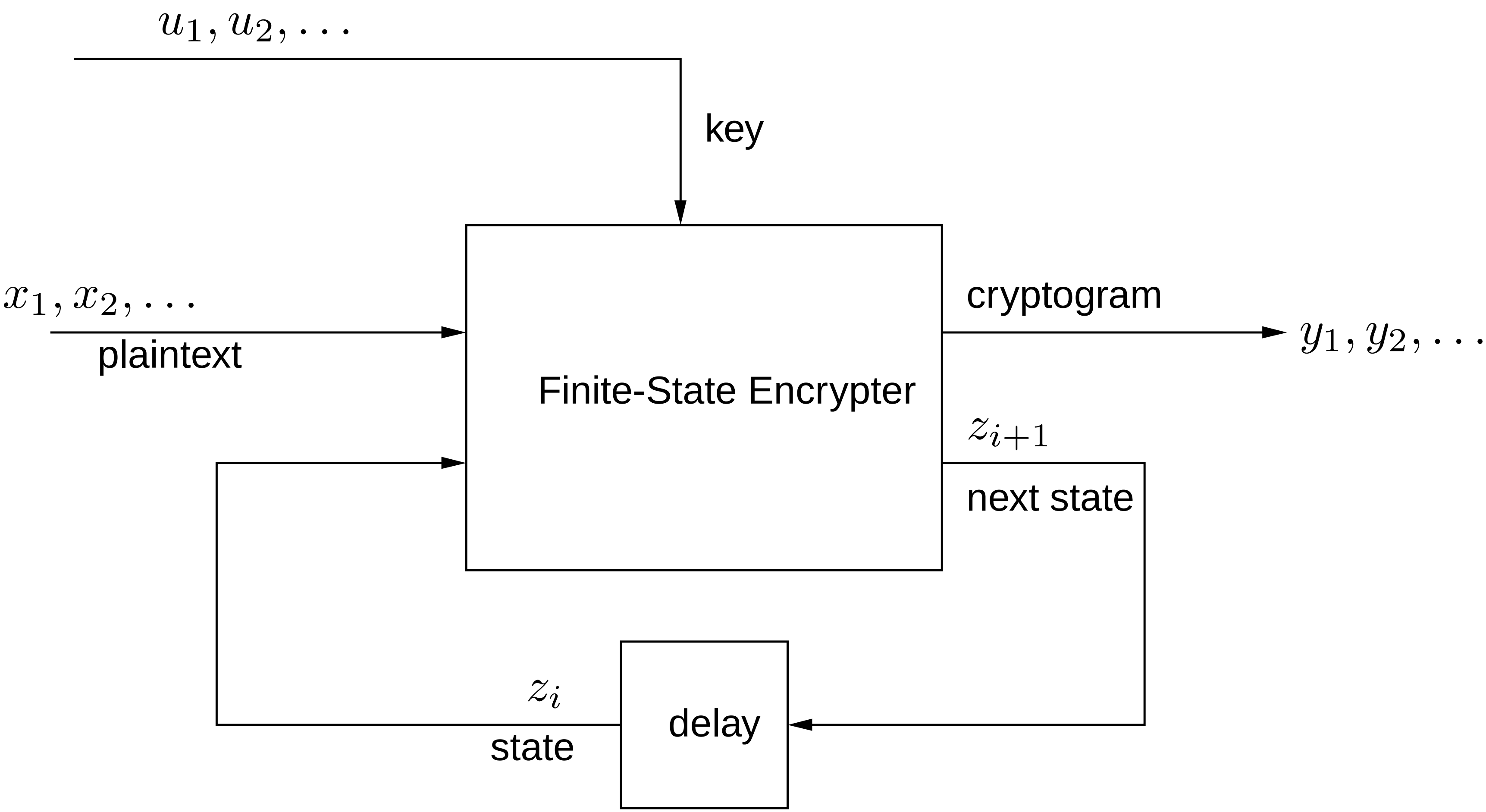
The only exception (a.f.a.i.k.) is an unpublished memorandum by Ziv [1978]:

- Plaintext source – individual sequence.
- Encrypter – general block encoder.
- Prior knowledge: plaintext $\rightarrow$ FSM $\rightarrow$ all–zero sequence.
- Full security: uncertainty – essentially not reduced by cryptogram.
- Main result: minimum needed key rate $\sim$ LZ compressibility.

Encrypter/decrypter have unlimited resources, whereas eavesdropper is limited by FSM.

Our approach: the other way around – encryption using FSM's.

Finite–State Encrypter Model



$$
\begin{aligned}
t_i &= t_{i-1} + \Delta(z_i, x_i), \qquad t_0 \triangleq 0 \\
k_i &= (u_{t_{i-1}+1}, u_{t_{i-1}+2}, \ldots, u_{t_i}) \\
y_i &= f(z_i, x_i, k_i) \\
z_{i+1} &= g(z_i, x_i)
\end{aligned}
$$

Finite–State Encrypter Model (Cont'd)

Perfect security: Pr$\{y^n|\boldsymbol{x}\}$ – independent of $\boldsymbol{x}$.

Information losslessness (IL): $\exists$ large n s.t. (z_1, z_{n+1}, k^n, y^n) determines x^n.

Key rate of encrypter E:

$$\sigma_E(x^n) = \frac{1}{n}\sum_{i=1}^{n}\Delta(z_i, x_i) = \frac{1}{n}\sum_{i=1}^{n}\ell(k_i).$$

$$\sigma_s(x^n) = \min_{E\in\mathcal{E}(s)}\sigma_E(x^n),$$

where $\mathcal{E}(s) =$ set of all perfectly secure, IL encrypters with $\leq s$ states.

$$\sigma_s(\boldsymbol{x}) = \limsup_{n\to\infty}\sigma_s(x^n)$$

Finite–state encryptability: $\sigma(\boldsymbol{x}) = \lim_{s\to\infty}\sigma_s(\boldsymbol{x})$.

Main Result

Let $\rho_{LZ}(x^n)$ denote the LZ compresion ratio, i.e.,

$$\rho_{LZ}(x^n) = \frac{c(x^n) \log c(x^n)}{n},$$

where $c(x^n)$ = number of LZ phrases in x^n.

Theorem (converse): For every x^n

$$\sigma_s(x^n) \geq \rho_{LZ}(x^n) - O\left(s \cdot \sqrt{\frac{\log(\log n)}{\log n}}\right).$$

Consequently,

$$\sigma(\boldsymbol{x}) \geq \rho(\boldsymbol{x}).$$

Discussion

- Direct: LZ compression + one–time pad encryption – $\sigma(\boldsymbol{x}) = \rho(\boldsymbol{x})$.
- Natural individual–sequence counterpart to the known probabilistic result.
- Same conclusion as in [Ziv78], although the model is different.
- Upperbound – lowerbound = $O(\sqrt{\log(\log n)/\log n})$.
- In compression – $O(1/\log n)$.

Main Ideas of Proof

Define joint empirical distribution of m–blocks of $(x^n, k^n, y^n, ...)$.

$$\sigma_E(x^n) = \frac{\ell(k^n)}{n} = \frac{H(K^m|L)}{m} \geq \frac{1}{m}[H(K^m) - \alpha s \log(m+1)].$$

Using usual information–theoretic arguments (+ IL + full security):

$$H(K^m) \geq H(X^m) - H(Z, Z'|Y^m, K^m) \geq H(X^m) - 2\log s.$$

Now, since Shannon code = FS encoder:

$$\frac{H(X^m)}{m} \geq \rho_{LZ}(x^n) - \delta_s(m, n).$$

So eventually,

$$\sigma_E(x^n) \geq \rho_{LZ}(x^n) - \text{vanishing terms.}$$

Extensions

Availability of Side Information

Assume that everybody has access to SI $s_1, s_2, \ldots$ (individual sequence). Modifying the model definition:

$$\begin{aligned} t_i &= t_{i-1} + \Delta(z_i, x_i, s_i), \qquad t_0 \stackrel{\Delta}{=} 0 \\ k_i &= (u_{t_{i-1}+1}, u_{t_{i-1}+2}, \ldots, u_{t_i}) \\ y_i &= f(z_i, x_i, k_i, s_i) \\ z_{i+1} &= g(z_i, x_i, s_i) \end{aligned}$$

Perfect security: Pr$(y^n|\boldsymbol{x}, \boldsymbol{s})$ – independent of $\boldsymbol{x}$.

Info losslessness: For large enough n: $(z_1, z_{n+1}, s^n, y^n, k^n)$ determine x^n.

Main result: Same but with $\rho_{LZ}(x^n)$ replaced by $\rho_{LZ}(x^n|s^n)$ – conditional LZ parsing of x^n given s^n [Ziv '85].

Achievable even if encrypter does not see s^n: S–W coding + one–time pad.

Availability of SI (Cont'd) – Conditional Parsing

- Apply LZ to $((x_1, s_1), (x_2, s_2), \ldots, (x_n, s_n))$; $c(x^n, s^n)$ = number of phrases.
- $c(s^n)$ = number of distinct phrases of s^n.
- $\boldsymbol{s}(l)$ = the lth distinct s–phrase, $l = 1, 2, ..., c(s^n)$.
- $c_l(x^n|s^n)$ = number of $\boldsymbol{s}(l)$ in parsing of s^n.

$$\rho_{LZ}(x^n|s^n) = \frac{1}{n} \sum_{l=1}^{c(s^n)} c_l(x^n|s^n) \log c_l(x^n|s^n).$$

For example,

$$\begin{aligned} x^6 &= 0 \mid 1 \mid 0\,0 \mid 0\,1| \\ s^6 &= 0 \mid 1 \mid 0\,1 \mid 0\,1| \end{aligned}$$

then

$$c(x^6, s^6) = 4, \;\; c(s^6) = 3, \;\; \boldsymbol{s}(1) = 0, \; \boldsymbol{s}(2) = 1, \; \boldsymbol{s}(3) = 01,$$

$$c_1(x^6|s^6) = c_2(x^6|s^6) = 1, \;\; c_3(x^6|s^6) = 2.$$

Lossy Reconstruction

Modifications in model definition:

- Legitimate reconstruction $\hat{x}^n$ must satisfy $d(x^n, \hat{x}^n) \leq nD$ w.p. 1.
- Distortion measure – completely arbitrary (need not be even additive).
- IL property can be relaxed to a weaker requirement (details in the paper).
- Perfect security: y^n is statistically independent of both $\boldsymbol{x}$ and $\hat{\boldsymbol{x}}$.

Main theorem essentially as before but $\rho_{LZ}(x^n)$ should be replaced by

$$r_{LZ}(D; x^n) = \min_{d(x^n, \hat{x}^n) \leq nD} \rho_{LZ}(\hat{x}^n).$$

- Not obvious that best $\hat{\boldsymbol{x}}^n$ is deterministic (could have depended on key).
- Achievability: again, conceptually obvious.
- In the full paper: also SI + lossy reconstruction; No longer based on LZ..

Thank You!