False–Accept/False–Reject Trade-offs for Ensembles of Biometric Authentication Systems

Neri Merhav

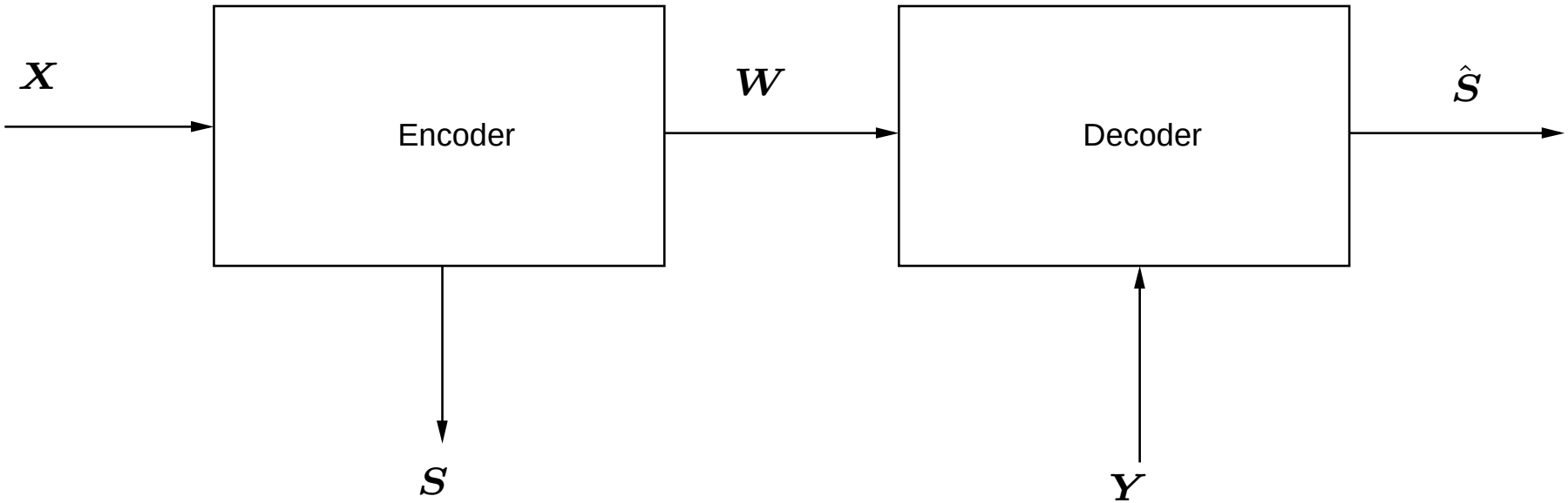
The Andrew & Erna Viterbi Faculty of Electrical Engineering

Technion—Israel Institute of Technology

Haifa 3200004, Israel

ISIT 2019, Paris, France, July 2019.

Block Diagram



- Encoding $\Leftrightarrow$ enrollment; X – biometric signal.
- S – secret key at rate R_{S}.
- W – helper message at rate R_{W}.
- Decoding $\Leftrightarrow$ authentication; Y – authentication signal.

Background, Motivation and Objectives

- Based on secret key generation: Csiszár & Ahlswede (1993, 1998); Maurer (1993).
- Ignateko & Willems (2010):
  - Small false accept (FA) rate.
  - Small false reject (FR) rate.
  - Small secrecy leakage, $I(\boldsymbol{S};\boldsymbol{W})/n$.
  - Small privacy leakage, $I(\boldsymbol{X};\boldsymbol{W})/n$.
- Achievable rates: $R_{\mathsf{S}} < I(X;Y)$; $H(X|Y) < R_{\mathsf{W}} < H(X) - R_{\mathsf{S}}$.

Achievability proofs – very rough bounds of FAR, FRR, and the leakages.

In an earlier work (M. 2018): exponential FA and FR error bounds.

Objectives: FA/FR trade–offs for FL/VL codes; optimal rate functions.

Model Setting

- $\{(X_i, Y_i))\}$ – memoryless process.
- Encoder: $\boldsymbol{w} = f(\boldsymbol{x}) \in \{1, 2, \ldots, e^{nR_{\mathsf{W}}}\}$, $\boldsymbol{s} = g(\boldsymbol{x}) \in \{1, 2, \ldots, e^{nR_{\mathsf{S}}}\}$
- Both f and g are selected at random (random binning).
- Decoder (authorized subscriber): $\hat{\boldsymbol{s}} = U(\boldsymbol{y}, \boldsymbol{w})$.
- Decoder (imposter): $\tilde{\boldsymbol{s}} = V(\boldsymbol{w})$.

Variable–rate: $R_{\mathsf{W}} = R_{\mathsf{W}}(Q_X)$, $R_{\mathsf{S}} = R_{\mathsf{S}}(Q_X)$, Q_X being the type of $\boldsymbol{x}$.

Decoders:

$$\hat{\boldsymbol{S}}_{\mathsf{MAP}} = \arg\max_{\boldsymbol{s}} P(\boldsymbol{s}, \boldsymbol{w}|\boldsymbol{y}) = \arg\max_{\boldsymbol{s}} \sum_{\boldsymbol{x}} P(\boldsymbol{x}|\boldsymbol{y}) \mathcal{I}\{f(\boldsymbol{x}) = w,\ g(\boldsymbol{x}) = s\}$$

$$\hat{\boldsymbol{S}}_{\mathsf{GLD}} \sim \tilde{P}(\boldsymbol{s}, \boldsymbol{w}|\boldsymbol{y}) \propto \sum_{\boldsymbol{x}} e^{na(\hat{P}_{\boldsymbol{xy}})} \mathcal{I}\{f(\boldsymbol{x}) = w,\ g(\boldsymbol{x}) = s\}$$

$$\tilde{\boldsymbol{S}}_{\mathsf{MAP}} = \arg\max_{\boldsymbol{s}} P(\boldsymbol{s}|\boldsymbol{w}).$$

Contributions

- Optimal rate functions for FL codes and VL codes.
- FA–FR trade–offs for both types of codes.
- Comparison between FL codes and VL codes.
- Privacy leakage.

We focus on the case of the optimal decoding metric.

Background [M. 2018]

The optimal FA exponent:

$$E_{\mathsf{FA}}(R_{\mathsf{w}}, R_{\mathsf{s}}) = \min_{Q_X}[D(Q_X\|P_X) + \min\{R_{\mathsf{s}}, [H_Q(X) - R_{\mathsf{w}}]_+\}]$$

The random–coding FR exponent:

$$E_{\mathsf{FR}}(R_{\mathsf{w}}) = \min_{Q_{XY}}\{D(Q_{XY}\|P_{XY}) + E(R_{\mathsf{w}}, Q_{XY})\},$$

where

$$E(R_{\mathsf{w}}, Q_{XY}) = \min_{Q_{X'|Y}}\{R_{\mathsf{w}} - H_Q(X'|Y) + [a(Q_{XY}) - a(Q_{X'Y})]_+\}.$$

Comments:

- FR exponent depends only on R_{w}, not on R_{s}.
- Identical to the error exponent of full decoding of $\boldsymbol{X}$ (Slepian–Wolf).
- $a(Q_{XY}) = -\beta H_Q(X|Y)$ is universally optimal for every $\beta \geq 1$.

Optimal Rate Functions for FL Codes

Necessary and sufficient conditions for $E_{\mathsf{FA}}(R_{\mathsf{W}}, R_{\mathsf{S}}) \geq E_0$ are:

- $R_{\mathsf{S}} \geq E_0$.
- $R_{\mathsf{W}} \leq R_{\mathsf{W}}(E_0)$

where

$$\begin{aligned} R_{\mathsf{W}}(E_0) &= \min\{-\mathbf{E}_Q \log P_X(X) - E_0 : \ D(Q_X \| P_X) \leq E_0\} \\ &= \sup_{\lambda \geq 0} \left\{ -\lambda \ln \left(\sum_x [P_X(x)]^{1+1/\lambda} \right) - (1+\lambda) E_0 \right\} \end{aligned}$$

Comments:

- $R_{\mathsf{S}} \geq E_0$ because even a blind guess succeeds w.p. $e^{-nR_{\mathsf{S}}}$.
- Second expression of $R_{\mathsf{W}}(E_0) =$ Rényi entropy of order $1 + 1/\lambda$.

Optimal Rate Functions for VL Codes

Necessary and sufficient conditions for achieving an FA exponent of E_0 are:

- $R_{\mathsf{s}}(Q_X) \geq R^*_{\mathsf{s}}(Q_X) \stackrel{\triangle}{=} E_0 - D(Q_X \| P_X)$.
- $R_{\mathsf{w}}(Q_X) \leq R^*_{\mathsf{w}}(Q_X)$,

where

$$R^*_{\mathsf{w}}(Q_X) \stackrel{\triangle}{=} \begin{cases} -\mathbf{E}_Q \ln P_X(X) & D(Q_X \| P_X) \leq E_0 \\ \infty & \text{otherwise} \end{cases}$$

FR/FA Error Exponent Trade-off: FL Codes

Since $E_{\mathsf{FR}}(R_{\mathsf{W}})$ is monotonically increasing in R_{W}, and since R_{W} cannot exceed $R^*_{\mathsf{W}}(E_0)$:

$$E^{\mathsf{f}}_{\mathsf{FR}}[E_0] = E_{\mathsf{FR}}(R^*_{\mathsf{W}}(E_0)) = \min_{Q_{XY}} \{D(Q_{XY} \| P_{XY}) + [R^*_{\mathsf{W}}(E_0) - H_Q(X|Y)]_+\}.$$

A Gallager–style expression:

$$E^{\mathsf{f}}_{\mathsf{FR}}[E_0] = \max_{0 \le \rho \le 1} \sup_{\lambda \ge 0} \left\{ -\ln \left[\sum_{y \in \mathcal{Y}} \left(\sum_{x \in \mathcal{X}} [P_{XY}(x,y)]^{1/(1+\rho)} \right)^{1+\rho} \right] - \rho\lambda \ln \left(\sum_{x \in \mathcal{X}} [P_X(x)]^{1+1/\lambda} \right) - \rho(1+\lambda)E_0 \right\}.$$

FR/FA Error Exponent Trade-off: VL Codes

$$E_{\mathsf{FR}}^{\mathsf{V}}[E_0] = \min_{\{Q_{XY}:\, D(Q_X\|P_X)\le E_0\}} \Bigg\{ D(Q_{XY}\|P_{XY}) + \Bigg[\mathbf{E}_Q \ln \frac{1}{P_X(X)} - E_0 - H_Q(X|Y) \Bigg]_+ \Bigg\},$$

or in its Gallager–style form:

$$E_{\mathsf{FR}}^{\mathsf{V}}[E_0] = \max_{0\le\lambda\le 1} \sup_{\rho\ge 0} \max_{V} \Big\{ -\ln M(V,\rho,\lambda) - (\rho+\lambda)E_0 \Big\},$$

where

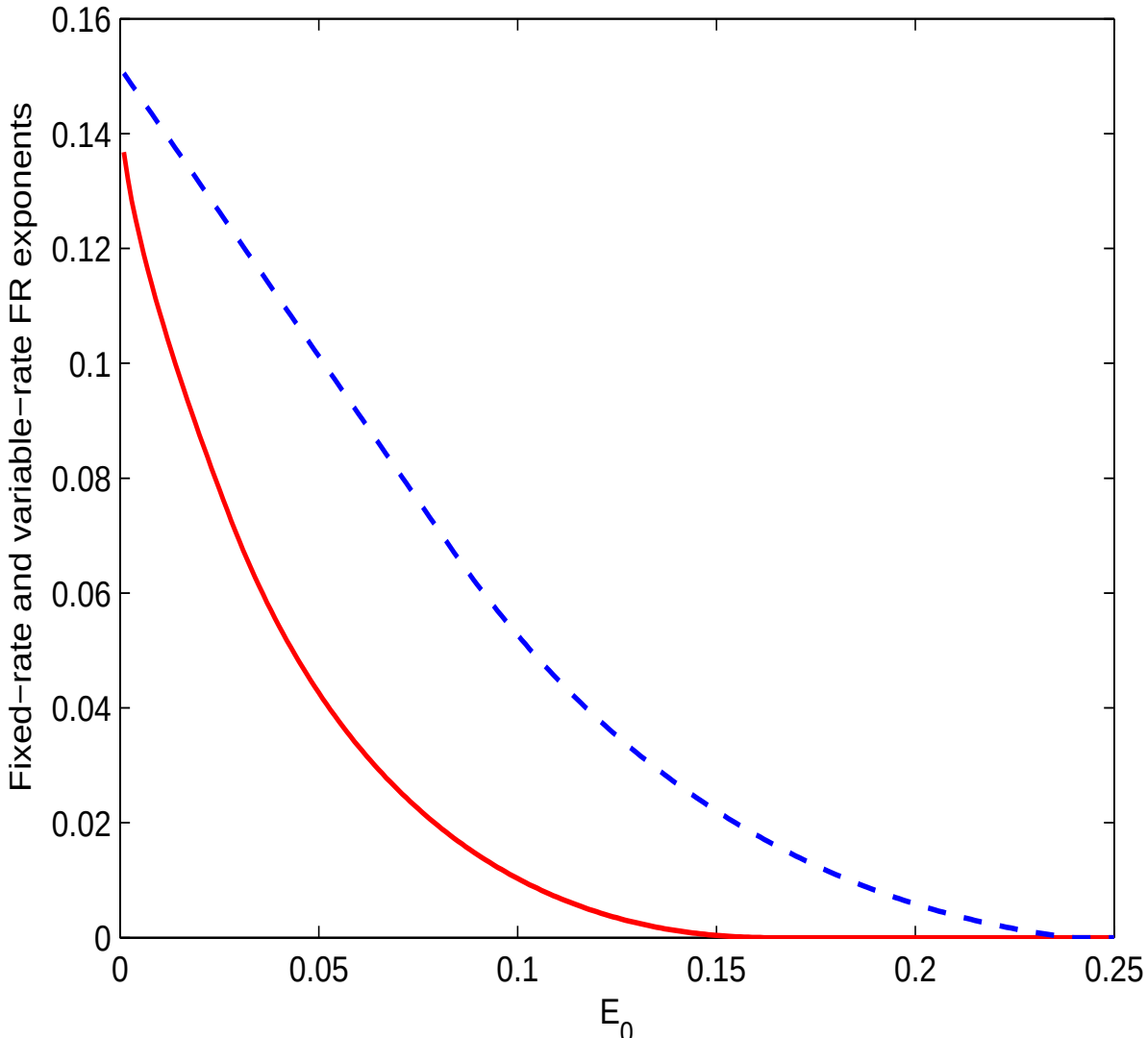
$$M(V,\rho,\lambda) = \sum_y \Bigg(\sum_x \Big[P_{XY}(x,y) P_X(x)^{\rho+\lambda} V(x)^{-\rho} \Big]^{1/(1+\lambda)} \Bigg)^{1+\lambda}.$$

Comment: Extension to mismatched decoding can be found in the paper.

A Numerical Example

The source:

$P_{XY}(0,0) = 0.32$, $P_{XY}(0,1) = 0.08$, $P_{XY}(1,0) = 0.06$, $P_{XY}(1,1) = 0.54$.



Privacy Leakage

The privacy leakage is defined as $I(\boldsymbol{X};\boldsymbol{W})$, which is equal to $H(\boldsymbol{W})$.
In the FL case, for the typical code,

$$H(\boldsymbol{W}) \leq n\left[R_{\mathsf{W}} + \min_{\{Q_X:\ H(Q_X)\geq R_{\mathsf{W}}\}} D(Q_X\|P_X)\right],$$

and so, if we require $H(\boldsymbol{W}) \leq nH_0$, then

$$R_{\mathsf{W}} \leq \min_{0\leq s\leq 1}\left\{\ln\left[\sum_{x\in\mathcal{X}} P_X^s(x)\right] + sH_0\right\}.$$

In the VL case, $H(\boldsymbol{W}) \leq nH_0$ can be satisfied as long as $H_0 \geq H_P(X) - E_0$.