Ensemble Performance of Biometric Authentication Systems Based on Secret Key Generation

Neri Merhav

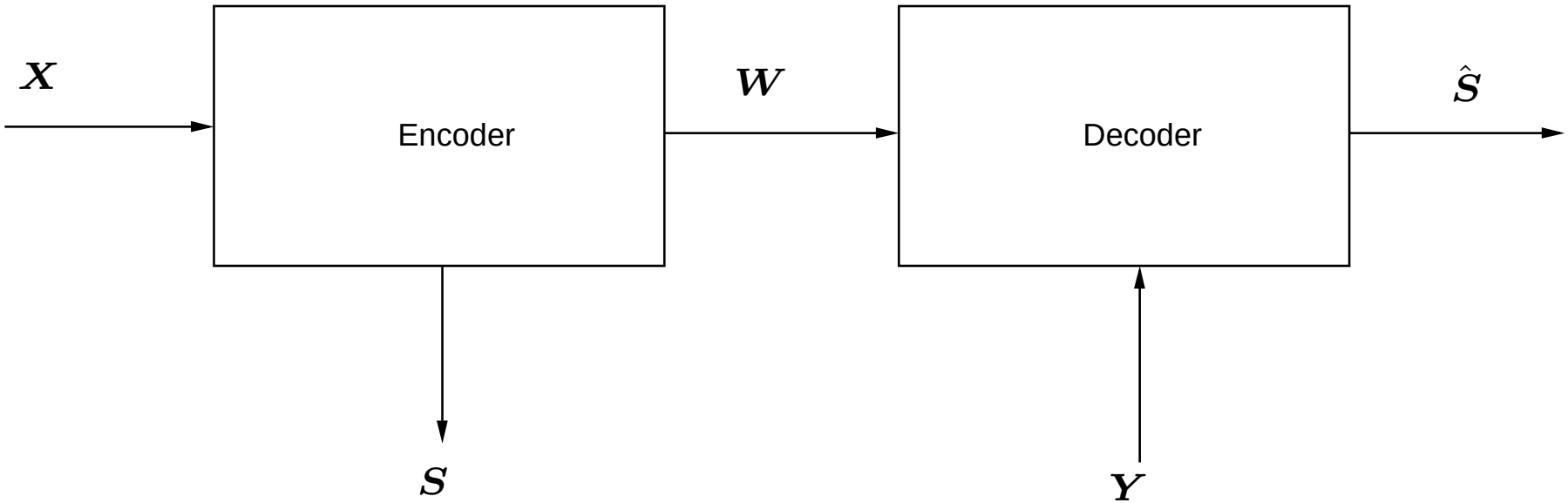
The Andrew & Erna Viterbi Faculty of Electrical Engineering

Technion—Israel Institute of Technology

Haifa 3200004, Israel

ISIT 2018, Vail, Colorado, U.S.A., June 2018.

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 common randomness: 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: $R_{\mathsf{S}} < I(X;Y)$; $H(X|Y) < R_{\mathsf{W}} < H(X) - R_{\mathsf{S}}$.

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

Objective: provide sharper evaluations as well as some lower bounds.

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): $\tilde{\boldsymbol{s}} = V(\boldsymbol{w})$.

Decoders:

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

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

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

Contributions

- FRR: exact random coding + expurgated exponent + converse bound.
- FAR: exact random coding exponent + fully matching converse bound.
- Secrecy leakage (exponentially decaying).
- Privacy leakage.

False Reject Rate: Random Coding Exponent

Defining

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

the exact random coding exponent is given by

$$E(R_{\mathsf{W}}) = \min_{Q_{XY}} [D(Q_{XY} \| P_{XY}) + E(R_{\mathsf{W}}, Q_{XY})].$$

Comments:

- 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 $\beta \geq 1$.
- Analysis using the type class enumeration method.

False Reject Rate: Expurgated Exponent

Define

$$\alpha(R_{\mathsf{W}}, Q_Y) = \sup_{\{Q_{X|Y}:\ H_Q(X|Y) > R_{\mathsf{W}}\}} [a(Q_{XY}) + H_Q(X|Y)] - R,$$

$$\gamma(Q_{XY}) = \max\{a(Q_{XY}, \alpha(R_{\mathsf{W}}, Q_Y)\},$$

and

$$\Lambda(Q_{XX'}) = \inf_{Q_{Y|XX''}} \{[\gamma(Q_{XY}) - a(Q_{X'Y})]_+ - H_Q(Y|XX') - \mathbf{E}_Q \ln P(Y|X)\},$$

the expurgated exponent is given by

$$E_{\mathsf{ex}}(R_{\mathsf{W}}) = \inf_{Q_{X'|X}:\ H_Q(X'|X) > R_{\mathsf{W}}\}} \{\Lambda(Q_{XX'}) - H_Q(X'|X) + R_{\mathsf{W}}\},$$

for almost every $\boldsymbol{x} \in \mathcal{T}(Q_X)$.

Discussion

- $\Lambda(Q_{XX'})$ plays the role of Bhattacharyya dist.
- Ensemble–tight in the exponential scale.
- At least as good as the random coding exponent at all rates.
- Exclusion of a minority of $\{\boldsymbol{x}\}$ from every type is justifiable.
- Analysis: type class enumeration plus concentration properties:

$$\mathbf{E}\{P_{\mathsf{FR}}^{1/\rho}\} = \mathbf{E}\left\{\sum_{\boldsymbol{s}\neq g(\boldsymbol{x})}\sum_{\boldsymbol{y}} P(\boldsymbol{y}|\boldsymbol{x})\frac{\tilde{P}(\boldsymbol{s},f(\boldsymbol{x})|\boldsymbol{y})}{e^{na(\hat{P}\boldsymbol{x}\boldsymbol{y})}+\sum_{\boldsymbol{x}'\neq\boldsymbol{x}} e^{na(\hat{P}\boldsymbol{x}'\boldsymbol{y})}\mathcal{I}[f(\boldsymbol{x}')=f(\boldsymbol{x})]}\right\}^{1/\rho}$$

The red expression concentrates very rapidly around $e^{n\alpha(R_{\mathsf{W}},Q_Y)}$.

Converse Bound

A lower bound in the spirit of the sphere–packing argument yields:

$$P_{\mathsf{FR}} \dot{\geq} \exp\left\{-n \inf_{Q_{XY}\in\mathcal{Q}} D(Q_{XY}\|P_{XY})\right\},$$

where

$$\mathcal{Q} = \{Q_{XY}:\ R_{\mathsf{W}} < H_Q(X|Y),\ R_{\mathsf{W}} + R_{\mathsf{S}} > H_Q(X)\}.$$

The bound is tight whenever $R_{\mathsf{S}} > H_{Q^*}(X) - R_{\mathsf{W}}$, Q^* being the minimizer of $D(Q_{XY}\|P_{XY})$ in the absence of the constraint $R_{\mathsf{W}} + R_{\mathsf{S}} > H_Q(X)$.

False Accept Rate: Random Coding Bound

The FA random coding bound is given by

$$E_{\mathsf{FA}}(R_{\mathsf{W}}, R_{\mathsf{S}}) = \inf_{Q_X} [D(Q_X \| P_X) + \min\{R_{\mathsf{S}}, [H_Q(X) - R_{\mathsf{W}}]_+\}.$$

Intuition: suppose that the imposter even knows $\mathcal{T}(Q_X)$:

- There are $e^{n[H_Q(X)-R_{\mathsf{W}}]_+}$ $\boldsymbol{x}$'s of type Q_X mapped to $\boldsymbol{w}$.
- $[H_Q(X) - R_{\mathsf{W}}]_+ > R_{\mathsf{S}}$: all $\boldsymbol{s}$ are equally likely.
- $[H_Q(X) - R_{\mathsf{W}}]_+ < R_{\mathsf{S}}$: $e^{n[H_Q(X)-R_{\mathsf{W}}]_+}$ distinct $\{\boldsymbol{s}\}$ appear.
- Gallager–style expression:

$$E_{\mathsf{FA}}(R_{\mathsf{W}}, R_{\mathsf{S}}) = \min_{0 \le s \le 1} \max_{s \le \rho \le 1} \left\{ -\rho \ln \left[\sum_x P(x)^{1/\rho} \right] + sR_{\mathsf{S}} - (1-\rho)R_{\mathsf{W}} \right\}.$$

- There is a matching converse bound.

Secrecy Leakage and Privacy Leakage

Secrecy Leakage:

For the typical code, $I(\boldsymbol{S};\boldsymbol{W}) \dot{\leq} \exp\{-nE_{\mathsf{sec}}(R_{\mathsf{s}}+R_{\mathsf{w}})\}$, where

$E_{\mathsf{sec}}(R) = \min\{D(Q\|P):\ H_Q(X) \leq R\}.$

Privacy Leakage:

Since $\boldsymbol{W} = f(\boldsymbol{X})$,

$$I(\boldsymbol{X};\boldsymbol{W}) = H(\boldsymbol{W}) \leq nR_{\mathsf{w}} + O\left(\frac{\log n}{n}\right),$$

and R_{w} can be chosen arbitrarily close (but above) $H(X|Y)$).

The cost of proximity is in compromising the FR exponent.