The Private Key Capacity Region for Three Terminals

Chunxuan Ye and Prakash Narayan
Department of Electrical and Computer Engineering
University of Maryland
College Park, MD 20742, U.S.A.
e-mail: {cxye, prakash}@eng.umd.edu

Abstract — **We consider a model with three terminals and examine the problem of characterizing the largest rates at which two pairs of terminals can simultaneously generate private keys, each of which is effectively concealed from the remaining terminal.**

I. Introduction

Suppose that terminals $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ observe, respectively, the distinct components of a discrete memoryless multiple source, i.e., i.i.d. repetitions of the random variables (rvs) X, Y, Z, respectively. The terminals are permitted unrestricted communication among themselves over a public channel, and all the transmissions are observed by all the terminals. An eavesdropper has access to this public communication but gathers no additional side information; also, the eavesdropper is passive, i.e., unable to corrupt the transmissions. Terminals $\mathcal{X}$ and $\mathcal{Y}$ (resp. $\mathcal{X}$ and $\mathcal{Z}$) generate a "private key" (PK) with the possible help of terminal $\mathcal{Z}$ (resp. $\mathcal{Y}$) which is concealed from the helper terminal $\mathcal{Z}$ (resp. $\mathcal{Y}$) and from an eavesdropper with access to the public communication among the terminals. Our main technical results are single-letter outer and inner bounds for the PK-capacity region. Further, under certain special conditions, for instance if the correlation of Y and Z is deterministic (i.e., there exists a common function of Y and Z which renders them conditionally independent), these bounds coincide to yield the PK-capacity region.

II. Statement of Results

Consider a discrete memoryless multiple source (DMMS) with three components corresponding to generic rvs X, Y, Z with finite alphabets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$. Let $X^n = (X_1, \cdots, X_n)$, $Y^n = (Y_1, \cdots, Y_n)$, $Z^n = (Z_1, \cdots, Z_n)$ be n i.i.d. repetitions of the rvs X, Y, Z. The terminals $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ respectively observe the components X^n, Y^n, Z^n of the DMMS (X^n, Y^n, Z^n), where n denotes the observation length. The terminals can communicate with each other through broadcasts over a noiseless public channel, possibly interactively in many rounds. Following [1], we assume without loss of generality that these transmissions occur in consecutive time slots in r rounds; the communication is depicted by $3r$ rvs $F_1, \cdots, F_{3r}$, where F_t denotes the transmission in time slot t, $1 \le t \le 3r$, by a terminal assigned an index $i = t \mod 3$, $1 \le i \le 3$, with terminals $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ corresponding to indices 1, 2, 3, respectively. In general, F_t is allowed to be any function, defined in terms of a mapping f_t, of the observations at the terminal with index i and of the previous transmissions $F^{t-1} = (F_1, \cdots, F_{t-1})$. Let $\mathbf{F}$ denote collectively all the transmissions. Randomization at the terminals is not permitted.

The rvs $K_{\mathcal{XY}}$, $L_{\mathcal{XY}}$ represent an ε-private key (ε-PK) for the terminals $\mathcal{X}$ and $\mathcal{Y}$ which is private from the helper terminal $\mathcal{Z}$, achievable with communication $\mathbf{F}$, if $K_{\mathcal{XY}}$ and $L_{\mathcal{XY}}$ are functions of the data available at terminals $\mathcal{X}$ and $\mathcal{Y}$, respectively, i.e., $K_{\mathcal{XY}} = K_{\mathcal{XY}}(X^n, \mathbf{F})$, $L_{\mathcal{XY}} = L_{\mathcal{XY}}(Y^n, \mathbf{F})$; $K_{\mathcal{XY}}$ and $L_{\mathcal{XY}}$ take values in the same finite set $\mathcal{K}_{\mathcal{XY}}$ with $\Pr\{K_{\mathcal{XY}} \ne L_{\mathcal{XY}}\} \le \varepsilon$; $K_{\mathcal{XY}}$ (or $L_{\mathcal{XY}}$) satisfies the *secrecy condition* $\frac{1}{n} I(K_{\mathcal{XY}} \wedge \mathbf{F}, Z^n) \le \varepsilon$; and $K_{\mathcal{XY}}$ (or $L_{\mathcal{XY}}$) satisfies the *uniformity condition* $\frac{1}{n} H(K_{\mathcal{XY}}) \ge \frac{1}{n} \log |\mathcal{K}_{\mathcal{XY}}| - \varepsilon$. We are interested in the *simultaneous generation* of individual PK pairs $(K_{\mathcal{XY}}, K_{\mathcal{XZ}})$ as above.

A pair of numbers $(R_{\mathcal{XY}}, R_{\mathcal{XZ}})$ is an *achievable PK-rate pair* if ε_n-PK pairs $(K^{(n)}_{\mathcal{XY}}, K^{(n)}_{\mathcal{XZ}})$ are achievable with suitable communication, such that $\varepsilon_n \to 0$, $\frac{1}{n} H(K^{(n)}_{\mathcal{XY}}) \to R_{\mathcal{XY}}$, $\frac{1}{n} H(K^{(n)}_{\mathcal{XZ}}) \to R_{\mathcal{XZ}}$. The set of all achievable PK-rate pairs is the *PK-capacity region* C_{PK}.

Our main results for the PK-capacity region are the following.

Theorem 1 (*Outer bound for* C_{PK}): Let $(R_{\mathcal{XY}}, R_{\mathcal{XZ}})$ be an achievable PK-rate pair. Then

$$R_{\mathcal{XY}} \le I(X \wedge Y|Z), \qquad R_{\mathcal{XZ}} \le I(X \wedge Z|Y), \tag{1}$$

$$R_{\mathcal{XY}} + R_{\mathcal{XZ}} \le I(X \wedge Y, Z) - \max_{U:\ U \multimap Y \multimap XZ,\ U \multimap Z \multimap XY} I(U \wedge X).$$

Theorem 2 (*Inner bound for* C_{PK}): The PK-capacity region C_{PK} is inner-bounded by the convex hull of the regions

$$\left\{ \begin{array}{ll} (R_{\mathcal{XY}}, R_{\mathcal{XZ}}): & 0 \le R_{\mathcal{XY}} \le I(X \wedge Y|U_{mss(Y)}, Z), \\ & 0 \le R_{\mathcal{XZ}} \le I(X \wedge Z|Y), \\ & R_{\mathcal{XY}} + R_{\mathcal{XZ}} \le I(X \wedge Y, Z) - I(U_{mss(Y)} \wedge X) \end{array} \right\}$$

and

$$\left\{ \begin{array}{ll} (R_{\mathcal{XY}}, R_{\mathcal{XZ}}): & 0 \le R_{\mathcal{XY}} \le I(X \wedge Y|Z), \\ & 0 \le R_{\mathcal{XZ}} \le I(X \wedge Z|V_{mss(Z)}, Y), \\ & R_{\mathcal{XY}} + R_{\mathcal{XZ}} \le I(X \wedge Y, Z) - I(V_{mss(Z)} \wedge X) \end{array} \right\},$$

where $U_{mss(Y)}$ (resp. $V_{mss(Z)}$) is the *minimal sufficient statistic* for Y (resp. Z) w.r.t. Z (resp. Y).

Theorem 3: If there exists a rv U such that

$$U \multimap Y \multimap XZ, \qquad U \multimap Z \multimap XY, \qquad Y \multimap U \multimap Z, \tag{2}$$

the PK-capacity region equals the set of pairs $(R_{\mathcal{XY}}, R_{\mathcal{XZ}})$ which satisfy (1) and

$$R_{\mathcal{XY}} + R_{\mathcal{XZ}} \le I(X \wedge Y, Z) - \max_{U} I(U \wedge X),$$

where the maximum is w.r.t. U satisfying (2).

Theorem 4: If Y and Z are *deterministically correlated*, the PK-capacity region C_{PK} equals the set of pairs $(R_{\mathcal{XY}}, R_{\mathcal{XZ}})$ which satisfy (1) and

$$R_{\mathcal{XY}} + R_{\mathcal{XZ}} \le I(X \wedge Y, Z) - I(U_{mcf} \wedge X),$$

where U_{mcf} is the *maximal common function* of Y and Z.

Reference

[1] I. Csiszár and P. Narayan, "The secret key capacity for multiple terminals," *IEEE Trans. Inform. Theory*, in review, 2003.