Authentication with Side Information

Wei Kang  Daming Cao
School of Information Science and Engineering
Southeast University
Nanjing, China 210096
Email: wkang@seu.edu.cn, dmcao@seu.edu.cn

Nan Liu
National Mobile Communications Research Laboratory
Southeast University
Nanjing, China 210096
Email: nanliu@seu.edu.cn

Abstract—In this paper, we study the probability of successful deception of an uncompressed biometric authentication system with side information at the adversary. It represents the scenario where the adversary may have correlated side information, e.g., a partial fingerprint or a DNA sequence of a relative of the legitimate user. We find the optimal exponent of the deception probability by proving both the achievability and the converse. Our proofs are based on the connection between the problem of deception with side information and the rate distortion problem with side information at both the encoder and decoder.

I. INTRODUCTION

The biometric authentication problem has been studied extensively in recent years. In a biometric authentication system, a biometric feature, e.g., a finger print, a DNA sequence, etc., of a legitimate user is measured and the measurement, called enrollment, is stored in the database. Later this biometric feature of the same user is measured and compared with the enrollment for authentication. Due to the randomness in the process, different measurements of the same biometric features of the same person can not be exactly the same. Thus, the authentication system has to tolerate a certain level of distortion between the enrollment and the measurement.

In a biometric authentication system, successful deception happens when an adversary impersonates a legitimate user by faking a biometric feature close enough to the enrollment and then deceives the authentication system. Thus, minimizing the probability of successful deception by the adversary is an important issue in the design of the biometric authentication system and the tolerated level of distortion. The first study on the deception probability in the biometric authentication system is [1], where the authors studied the deception in an authentication system where the enrollment is compressed. The authors obtained the optimal trade-off between the compression rate and the exponent of the probability of successful deception when the adversary has no side information. In the case with correlated side information at the adversary, achievability and converse results on the optimal trade-off were proposed in the paper, however, they do not meet. A similar result was obtained in a recent paper [2], where the optimal exponent of the deception probability has been given in both cases of uncompressed and compressed enrollment with no side information at the adversary.

A different direction in studying the performance of a biometric authentication system is to study the maximum number of legitimate users allowed in a biometric authentication system under a given tolerated distortion level. In [3], the capacity, i.e., the maximum number of legitimate users, is obtained if the enrollment data is not compressed. Later, the capacity result is generalized to the case where the enrollment data is compressed [4], and the trade-off between the compression rate and the capacity of the authentication system was studied. The threat of a deception from an adversary was not considered in this line of work.

In this paper, we study the optimal exponent of the probability of successful deception of a biometric authentication system with uncompressed enrollment and side information at the adversary. It represents the scenario where the adversary may have correlated side information, e.g., a partial fingerprint of the legitimate user or a DNA sequence of a relative of the legitimate user. We find the optimal exponent of the deception probability by providing the proofs of both the achievability and the converse. Our proofs are based on a connection between the problem of deception with side information and the rate distortion problem with side information at both the encoder and decoder.

II. PROBLEM FORMULATION AND MAIN RESULT

A. Problem Formulation

Consider a pair of independent and identically distributed (i.i.d.) random sequences $X^n$ and $Y^n$, generated according to a joint distribution $P$, which is defined on a finite space $\mathcal{X} \times \mathcal{Y}$. Th random sequence $X^n$ represents the biometric enrollment in the system and $Y^n$ represents the side information at the adversary. We define a reconstruction space $\hat{\mathcal{X}}$ and a distortion function $d : \mathcal{X} \times \hat{\mathcal{X}} \to \mathbb{R}^+ \cup \{0\}$. The distortion between the sequences $x^n \in \mathcal{X}^n$ and $\hat{x}^n \in \hat{\mathcal{X}}^n$ is defined as

$$d(x^n, \hat{x}^n) \triangleq \frac{1}{n} \sum_{i=1}^{n} d(x_i, \hat{x}_i). \tag{1}$$

The legitimate user is successfully identified if the distortion between the measurement in the authentication stage and the
enrollment does not exceed a certain level, say \( \Delta \). The adversary observes the side information \( Y^n \) and tries to impersonate the legitimate user using a deception function \( f : \mathcal{Y}^n \mapsto \hat{X}^n \). We define the achievable deception exponent as follows.

**Definition 1** A deception exponent \( E \) is achievable under the distortion constraint \( \Delta \) if there exists a deception function \( f \) such that

\[
-\frac{1}{n} \log \Pr(d(X^n, f(Y^n)) \leq \Delta + \delta) \leq E + \delta
\]

In this paper, we are interested in the minimal achievable deception exponent, which is the best the adversary can do. Based on the minimal achievable deception exponent, the designer of the biometric authentication system can choose an appropriate \( \Delta \) value that on one hand, limit the probability of successful deception to a tolerate level, and on the other hand, does not cause too large a probability of false-rejection when the legitimate user is authenticated [2].

**B. Rate-distortion with Side Information at Both the Encoder and Decoder**

It turns out that finding the minimal achievable deception exponent with side information at the adversary is intimately related to the rate distortion problem with side information at both the encoder and decoder [5]. Thus, in this subsection, we review the results for this rate distortion problem.

Assume a pair of i.i.d sequences \( X^n \) and \( Y^n \) generated according a joint distribution \( Q \) defined on \( \mathcal{X} \times \mathcal{Y} \), where \( Q \) is not necessarily equal to \( P \), defined in the previous subsection. The random sequence \( X^n \) is the source sequence to be reconstructed at the decoder with a certain distortion constraint and \( Y^n \) represents the side information available at both the encoder and decoder. Thus, the encoding function at the encoder is defined as \( g : \mathcal{X}^n \times \mathcal{Y}^n \mapsto \{1, 2, \ldots, M\} \), and the decoding function at the decoder is defined as \( \varphi : \{1, 2, \ldots, M\} \times \mathcal{Y}^n \mapsto \hat{X}^n \). We denote the minimal achievable rate under distortion constraint \( \Delta \) in the rate distortion problem with side information at both the encoder and decoder as \( R_{SI}(Q, \Delta) \). From [5], we have

\[
R_{SI}(Q, \Delta) = \min_{V(\hat{x}|x,y):E(d(X,\hat{X})) \leq \Delta} I(X; \hat{X}|Y) \quad (3)
\]

**Remark:** The above rate distortion problem with side information at both the encoder and decoder can also be viewed as a special case of the Wyner-Ziv problem, i.e., the rate distortion problem with side information only at the decoder, as follows: in the Wyner-Ziv problem, view \( (X^n, Y^n) \) jointly as the source sequence available at the encoder, view \( Y^n \) as the side information at the decoder, and take the distortion function in the Wyner-Ziv problem as \( d(x, \hat{x}) \), which is defined in the previous subsection. By viewing the rate distortion problem with side information at both the encoder and decoder as a special case of the Wyner-Ziv problem, we can invoke the results of the Wyner-Ziv problem, e.g., [6, Theorem 16.5] in later development.

**C. Main Result**

The main result of this paper is the following theorem.

**Theorem 1** The deception exponent \( E \) is achievable under the distortion constraint \( \Delta \) if and only if

\[
E \geq \min_Q \{D(Q||P) + R_{SI}(Q, \Delta)\} \quad (4)
\]

where \( R_{SI}(Q, \Delta) \) is given in (3).

In the next two sections, we will show the proofs of the achievability and the converse of Theorem 1 via the connection between the problem of deception with side information and the rate distortion problem with side information at both the encoder and decoder.

**III. The Achievability**

In this section, we will show that for any distribution \( Q \) defined on \( \mathcal{X} \times \mathcal{Y} \), there exists a deception function \( f \) that can achieve the the deception exponent \( D(Q||P) + R_{SI}(Q, \Delta) \) under the distortion constraint \( \Delta \). We will construct the deception function \( f \) from the rate distortion code with side information at both the encoder and decoder.

First, consider the rate distortion problem with side information at both the encoder and decoder as defined in subsection II-B, where \( (X^n, Y^n) \) generated i.i.d. according to an arbitrary distribution \( Q \). Theorem 16.5 in [6] shows that for any sufficiently large \( n \), and \( 0 < \tau < 1 \), there exists a length \( n \) code that achieves rate \( R_{SI}(Q, \Delta) \) and satisfies the distortion constraint with probability larger than \( 1 - \tau \). More specifically, there exists a function pair \((g, \varphi)\) such that

\[
\frac{1}{n} \log \|g\| \leq R_{SI}(Q, \Delta) + \delta
\]

\[
\Pr(d(X^n, \varphi(g(X^n, Y^n)), Y^n)) \leq \Delta + \delta > 1 - \tau
\]

We will derive some properties of the function pair \((g, \varphi)\) in the following. Define \( A \subset \mathcal{X}^n \times \mathcal{Y}^n \) as the set of sequences \((x^n, y^n)\) that satisfies the distortion constraint \( \Delta + \delta \) under \((g, \varphi)\), i.e.,

\[
A \triangleq \{(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n : d(x^n, \varphi(g(x^n, y^n)), y^n) \leq \Delta + \delta\}
\]

Thus, (6) is equivalent to

\[
Q^n(A) > 1 - \tau
\]

We further define \( A(Q) \) as the intersection of the set \( A \) with the typical set \( T^n_{[Q]_S} \), defined in [6, Definition 2.8], i.e.,

\[
A(Q) \triangleq A \cap T^n_{[Q]_S}
\]

From the property of the typical set, we have

\[
Q^n(T^n_{[Q]_S}) \geq 1 - \epsilon_n,
\]

and as a result, from (8) and (10), we have

\[
Q^n(A(Q)) > 1 - \epsilon_n - \tau
\]
Thus, using [6, Lemma 2.14], we have
\[ \frac{1}{n} \log |A(Q)| \geq H(Q) - \epsilon_n \] (12)
We further define \( A_i(Q) \subset A(Q) \) for \( i = 1, 2, \ldots, |g| \) as the set of \((x^n, y^n)\) sequences that when mapped to index \( i \) at the encoder satisfy the distortion constraint, i.e.,
\[ A_i(Q) = \{ (x^n, y^n) \in T_Q^{(i)} : d(x^n, y^n) \leq \Delta + \delta \} \] (13)
Since all \((x^n, y^n)\) sequences that satisfy the distortion constraint \( \Delta + \delta \) under \((g, \varphi)\) has to be mapped to an index \( g(x^n, y^n) \), we have
\[ A(Q) = \bigcup_{i=1}^{|g|} A_i(Q) \] (14)
There exists an \( i \in \{1, 2, \ldots, |g|\} \), denoted by \( i^o \), such that
\[ |A_{i^o}(Q)| \geq \frac{|A(Q)|}{|g|} \] (15)
Therefore, we have
\[ -\frac{1}{n} \log P^n(A_{i^o}(Q)) \leq -\frac{1}{n} \log \left( \min_{(x^n, y^n) \in A_{i^o}(Q)} P^n((x^n, y^n)) \right) \]
\[ \leq -\frac{1}{n} \log \left( \frac{|A(Q)|}{|g|} \min_{(x^n, y^n) \in A_{i^o}(Q)} P^n((x^n, y^n)) \right) \]
\[ \leq -H(Q) + \epsilon_n + R_{ST}(Q, \Delta) + \delta \]
\[ \leq -H(Q) + \epsilon_n + R_{ST}(Q, \Delta) + \delta + D(Q) + H(Q) + \epsilon_n \]
\[ = D(Q) + R_{ST}(Q, \Delta) + \delta + 2\epsilon_n \] (19)
where (16) follows from (15), (17) follows from (5) and (12), and (18) follows from [6, Lemma 2.6], i.e., for any \((x^n, y^n) \in T_Q^{(i^o)}\),
\[ -\frac{1}{n} \log P^n((x^n, y^n)) \leq D(Q) + H(Q) + \epsilon_n \] (20)
Now, we are ready to construct the deception function \( f \) according to \((g, \varphi)\) described above, i.e.,
\[ f(y^n) = \varphi(i^o, y^n) \] (21)
Then we have
\[ -\frac{1}{n} \log \Pr(d(X^n, f(Y^n)) \leq \Delta + \delta) \]
\[ = -\frac{1}{n} \log P^n((x^n, y^n) : d(x^n, \varphi(i^o, y^n) \leq \Delta + \delta)) \] (22)
\[ \leq -\frac{1}{n} \log P^n(A_{i^o}(Q)) \]
\[ \leq D(Q) + R_{ST}(Q, \Delta) + \delta + 2\epsilon_n \] (23)
where (22) follows from the construction of \( f \) in (21), (23) follows from the definition of \( A_i(Q) \) in (13), and (24) follows from the properties of \((g, \varphi)\) we derived in (19).
Thus, we have shown that for any distribution \( Q \) defined on \( \mathcal{X} \times \mathcal{Y} \), there exists a deception function \( f \), constructed according to the encoding and decoding function of the corresponding rate distortion problem with side information, that can achieve the the deception exponent \( D(Q) + R_{ST}(Q, \Delta) \) under the distortion constraint \( \Delta \). This concludes the proof of the achievability.

IV. THE CONVERSE

In this section, we will prove that for any deception function \( f \), the deception exponent cannot be smaller than \( \min_Q \{ D(Q) + R_{ST}(Q, \Delta) \} \). This will be proven by contradiction, i.e., we will show that if there is a deception function with deception exponent equal to \( \min_Q \{ D(Q) + R_{ST}(Q, \Delta) \} - \alpha \) for some \( \alpha > 0 \), then we can construct a coding scheme in the rate distortion with side information problem with achievable rate smaller than \( R_{ST}(Q, \Delta) \), which is obviously false. The converse proof include the following three steps.

Step 1 Type selection: Assume a deception function \( f \), which achieves the deception exponent \( E \) under distortion constraint \( \Delta \), as defined in (2).

We define a set \( A \subset \mathcal{X}^n \times \mathcal{Y}^n \) as follows
\[ A = \{ (x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n : d(x^n, f(y^n)) \leq \Delta + \delta \} \] (25)
Then based on the definition of set \( A \), (2) is the same as saying
\[ -\frac{1}{n} \log P^n(A) \leq E + \delta \] (26)
For any distribution \( Q \) on \( \mathcal{X} \times \mathcal{Y} \), we define the set \( A(Q) \) as the intersection between the set \( A \) and \( T_Q^n \), where \( T_Q^n \) is the type of \( Q \) as defined in [6, Definition 2.1], i.e.,
\[ A(Q) = A \cap T_Q^n \] (27)
Thus, we have
\[ A = \bigcup_Q A(Q) \] (28)
and since the set \( T_Q^n \), and hence \( A(Q) \), for different distribution \( Q \) are disjoint, we have
\[ P^n(A) = \sum_Q P^n(A(Q)) \] (29)
Let \( \beta \) by the number of different types in \( \mathcal{X}^n \times \mathcal{Y}^n \). From (29), there exists a type \( Q^o \) such that
\[ P^n(A(Q^o)) \geq \frac{P^n(A)}{\beta} \] (30)
Thus, we have
\[ -\frac{1}{n} \log P^n(A(Q^o)) \leq -\frac{1}{n} \log \frac{P^n(A)}{\beta} \]
\[ \leq E + \delta + \frac{1}{n} \log \beta \] (31)
\[ < E + \epsilon_n + \delta \] (32)
where (31) follows from (26), and (32) follows from the fact that $\beta \leq (n+1)^{-|\mathcal{Y}|}\lambda^{|\mathcal{Y}|}$ [6, Lemma 2.2].

Since every sequence in the same type is equally probable, we have

$$P^n(A(Q^n)) = |A(Q)|P^n(x^n, y^n), \quad \forall(x^n, y^n) \in \mathcal{T}_Q^n$$

(33)

Thus, for any sequence pair $(x^n, y^n) \in \mathcal{T}_Q^n$, we have

$$\frac{1}{n} \log |A(Q^n)| = \frac{1}{n} \log \frac{P^n(A(Q^n))}{P^n(x^n, y^n)}$$

$$> -E - \epsilon_n - \delta - \frac{1}{n} \log P^n((x^n, y^n))$$

(34)

$$= D(Q^n||P) + H(Q^n) - E - \epsilon_n - \delta$$

(35)

where (34) follows from (32), and (35) follows from [6, Lemma 2.6], i.e., for any distribution $Q$, 

$$-\frac{1}{n} \log P^n((x^n, y^n)) = D(Q||P) + H(Q), \quad \forall(x^n, y^n) \in \mathcal{T}_Q^n$$

Step 2 Permutation: We will construct a rate distortion code with side information at both the encoder and decoder from the above deception function $f$ via permutations. We consider the symmetric group $S_n$, which consists of all the permutations on $\{1, 2, \ldots, n\}$. For a set $S \subset \mathcal{X}^n$, and a permutation $\pi \in S_n$, define the set $\pi(S)$ as the set of sequences that is permuted from the set $S$ via the permutation $\pi$, i.e.,

$$\pi(S) \triangleq \{x^n \in \mathcal{X}^n : \exists x^n \in S, \pi(x^n) = x^n\}$$

(36)

Thus, $\pi(S)$ is a permuted version of the set $S$. We will use the following lemma to obtain a covering of $\mathcal{T}_Q^n$ via $A(Q^n)$.

Lemma 1 (Covering Lemma) [7, Section 6.1] For any set $S \in \mathcal{T}_Q^n$, there exist permutations $\pi_1, \pi_2, \ldots, \pi_k \in S_n$ with

$$\bigcup_{i=1}^{k} \pi_i(S) = \mathcal{T}_Q^n$$

(37)

if

$$k > \frac{|\mathcal{T}_Q^n|}{|S|} \log |\mathcal{T}_Q^n|$$

(38)

In the above lemma, let $Q$ be $Q^n$ and $S$ be $A(Q^n)$, we have

$$\bigcup_{i=1}^{k} \pi_i(A(Q^n)) = \mathcal{T}_Q^n$$

(39)

where $k$ satisfies

$$\frac{1}{n} \log k$$

$$= \frac{1}{n} \log |\mathcal{T}_Q^n| - \frac{1}{n} \log |A(Q^n)| - \log (\log |\mathcal{T}_Q^n|) + \epsilon_n$$

$$\leq E - D(Q^n||P) + 2\epsilon_n + \delta + \frac{\log(nH(Q^n))}{n}$$

(40)

where (40) follows from (35) and the fact that the size of the type $|\mathcal{T}_Q^n|$ satisfies [6, Lemma 2.3]

$$(n+1)^{-|\mathcal{Y}|}\lambda^{|\mathcal{Y}|} \exp(nH(Q^n)) \leq |\mathcal{T}_Q^n| \leq \exp(nH(Q^n))$$

Based on (1), (25) and (27), we have that for $i = 1, 2, \ldots, k$

$$d(x^n, y^n) \leq \Delta + \delta, \quad \text{for every } (x^n, y^n) \in \pi_i(A(Q^n))$$

(41)

Thus, we can view the set $\pi_i(A(Q^n))$ as

$$\pi_i(A(Q^n)) = \{(x^n, y^n) \in \mathcal{T}_Q^n : d(x^n, \pi_i(f(\pi_i^{-1}(y^n)))) \leq \Delta + \delta\}$$

(42)

From (39), we know that the sets $\pi_i(A(Q^n))$, $i = 1, 2, \ldots, k$ form a covering of the type $\mathcal{T}_Q^n$. Therefore, for the rate distortion problem with side information at the encoder and decoder where $(X^n, Y^n)$ are generated i.i.d. according to distribution $Q^n$, we can construct an encoding-decoding pair $(g, \phi)$ based on the deception function $f$ as follows for $(x^n, y^n) \in \mathcal{T}_Q^n$. We define $g(x^n, y^n) = i$ if $(x^n, y^n) \in \pi_i(A(Q^n))$. If there exist multiple sets $\pi_i(A(Q^n))$ in which $(x^n, y^n)$ belongs, we can arbitrarily pick one set and assign the index of that set to the output of the function $g$. Define $Q^n_\phi$ as the marginal distribution of $Q^n$ in $\mathcal{Y}$. Then, for $i = 1, 2, \ldots, k$ and $y^n \in \mathcal{T}_{Q^n_\phi}$, we define the decoding function $\phi$ as follows

$$\phi(i, y^n) = \pi_i(f(\pi_i^{-1}(y^n)))$$

(43)

Thus, we obtain a code $(g, \phi)$ for the rate-distortion problem with side information available at both the encoder and decoder for every $(x^n, y^n) \in \mathcal{T}_Q^n$, which satisfies

$$||g|| = k$$

(44)

$$d(x^n, \phi(g(x^n, y^n), y^n)) \leq \Delta + \delta$$

(45)

Step 3 Expansion: In the previous step, we have construct a code $(g, \phi)$ for the type $\mathcal{T}_Q^n$. In this step, we will expand the code, first to the typical set $\mathcal{T}_Q^n$, and then to the whole space $\mathcal{X}^n \times \mathcal{Y}^n$.

Definition 2 [6, Chapter 5] Given a set $S \subset \mathcal{X}^n \times \mathcal{Y}^n$, we define the Hamming $\delta$ neighborhood of $S$ as

$$\Gamma^\delta(S) \triangleq \{(x^n, y^n) : \exists (x^n, y^n) \in S : d_H((x^n, y^n), (x^n, y^n)) \leq \delta\}$$

(46)

where $d_H$ represents the Hamming distance between two sequence pairs, i.e., the number of positions in which these two sequence pairs differ divided by $n$.

Based on the above definition, we have

$$\mathcal{T}_{[Q^n],k} \subset \bigcap_{i=1}^{k} \Gamma^{|\mathcal{Y}|\delta}(\mathcal{T}_Q^n) = \bigcup_{i=1}^{k} \Gamma^{|\mathcal{Y}|\delta}(\pi_i(A(Q^n)))$$

(47)

We construct the encoding function $g$ on the set $\Gamma^{|\mathcal{Y}|\delta}(\mathcal{T}_Q^n)$ in a similar way as we constructed the function $g$ on the type $\mathcal{T}_Q^n$ in the previous step. More specifically, we define $g(x^n, y^n) = i$ if $(x^n, y^n) \in \Gamma^{|\mathcal{Y}|\delta}(\pi_i(A(Q^n)))$. If there exist multiple sets $\Gamma^{|\mathcal{Y}|\delta}(\pi_i(A(Q^n)))$ in which
an arbitrary sequence in $\hat{g}$ analysis, we have that

\[
\mathcal{T}_{\hat{g}}^n \to \mathcal{T}_{Q^n}^n \text{ to the set } \Gamma^{X||Y|\delta}(\mathcal{T}_{Q^n}^n).
\]

For $y^n \in \Gamma^{X||Y|\delta}(\mathcal{T}_{Q^n}^n)$, we find a sequence $\tilde{y}^n$ in the type $\mathcal{T}_{\hat{g}}^n$ which has smallest Hamming distance with $y^n$. We then define $\varphi(i, y^n) = \varphi(i, \tilde{y}^n)$ for $i = 1, 2, \ldots, k$. If there are multiple $\tilde{y}^n$ sequences satisfying the above condition, we select one arbitrarily.

Now, for every $(x^n, y^n) \in \Gamma^{X||Y|\delta}(\pi_i(A(Q^n)))$, but not in $\mathcal{T}_{Q^n}$, there exists a $(\tilde{x}^n, \tilde{y}^n) \in \pi_i(A(Q^n))$ such that

\[
d_H((x^n, y^n), (\tilde{x}^n, \tilde{y}^n)) \leq n|X||Y|\delta
\]

and from the definition of $\pi_i(A(Q^n))$ we know that

\[
d(\tilde{x}^n, \pi_i(f(\pi_i^{-1}(\tilde{y}^n)))) \leq \Delta + \delta
\]

Therefore, we have

\[
d(x^n, \varphi(i, y^n)) = d(x^n, \varphi(i, \tilde{y}^n)) \leq d(\tilde{x}^n, \varphi(i, \tilde{y}^n)) + d_M|X||Y|\delta
\]

where

\[
d_M \triangleq \max_{x,\hat{x} \in X \times \hat{X}} d(x, \hat{x})
\]

With the above definition of $(g, \varphi)$ on $\Gamma^{X||Y|\delta}(\mathcal{T}_{Q^n}^n)$ and the analysis, we have that

\[
||g|| = k
\]

\[
d(x^n, \varphi(g(x^n, y^n), y^n)) \leq \Delta + \delta + d_M|X||Y|\delta
\]

(53) follows from (49) and (50).

Finally, we expand the rate-distortion code $(g, \varphi)$ to all $(x^n, y^n) \in X^n \times Y^n$. For $(x^n, y^n) \notin \Gamma^{X||Y|\delta}(\mathcal{T}_{Q^n}^n)$, we define $g(x^n, y^n) = 1$. For $y^n \notin \Gamma^{X||Y|\delta}(\mathcal{T}_{Q^n}^n)$, $\varphi(i, y^n)$ is an arbitrary sequence in $X^n$ for every $i$.

Therefore, we have for $(g, \varphi)$ defined on $X^n \times Y^n$

\[
\frac{1}{n} \log ||g|| \leq E - D(Q^n||P) + 2\epsilon_n + \delta + \log(nH(Q^n))
\]

\[
\text{Pr}(d(x^n, \varphi(g(x^n, y^n), y^n)) \leq \Delta + \delta + d_M|X||Y|\delta) \geq 1 - \frac{|X||Y|}{4n\delta^2}
\]

(54) follows from (40), and (55) follows from (50) and the fact that [6, Lemma 2.12]

\[
(Q^n)^n(\mathcal{T}_{Q^n}^n) \geq 1 - \frac{|X||Y|}{4n\delta^2}
\]

The inequality in (55) leads to

\[
E(d(X^n, \varphi(g(X^n, Y^n), Y^n))) \leq \Delta + \delta + d_M|X||Y|\delta + d_M|X||Y|\frac{1}{4n\delta^2}
\]

Thus, if we have a deception function, which under the distortion constraint $\Delta$ can achieve the deception exponent

\[
E = \min_Q D(Q||P) + R_{SI}(Q, \Delta) - \alpha
\]

for some $\alpha > 0$, then we can construct a rate distortion code with side information at both the encoder and decoder, where $(X^n, Y^n)$ is generated i.i.d. according to the distribution $Q^n$, that satisfies

\[
\frac{1}{n} \log ||g|| \leq \min_Q \{D(Q||P) + R_{SI}(Q, \Delta)\} - \alpha
\]

\[
- D(Q^n||P) + 2\epsilon_n + \frac{\log(nH(Q^n))}{n} \leq R_{SI}(Q^n, \Delta) - \alpha + 2\epsilon_n + \frac{\log(nH(Q^n))}{n}
\]

(59)

and

\[
E(d(X^n, \varphi(g(X^n, Y^n), Y^n))) \leq \Delta + \delta + d_M|X||Y|\delta + d_M|X||Y|\frac{1}{4n\delta^2}
\]

(60)

Since the rate distortion function $R_{SI}(Q^n, \Delta)$ is a continuous function of $\Delta$, the above result contradicts with the result in the rate distortion problem with side information at both encoder and decoder. This concludes the proof of the converse.

V. Conclusion

In this paper, we studied the probability of successful deception of an uncompressed biometric authentication system with side information at the adversary. We find the optimal exponent of the deception probability by providing the proofs of both the achievability and the converse. The results are proved by exploiting a connection between the problem of deception with side information and the rate distortion problem with side information at both the encoder and decoder.

REFERENCES


