On the Information-Theoretic Security of Combinatorial All-or-Nothing Transforms

Yujie Gu, Member, IEEE, Sonata Akao, Navid Nasr Esfahani, Ying Miao, and Kouichi Sakurai, Member, IEEE

Abstract—All-or-nothing transforms (AONTs) were proposed by Rivest as a message preprocessing technique for encrypting data to protect against brute-force attacks, and have numerous applications in cryptography and information security. Later the unconditionally secure AONTs and their combinatorial characterization were introduced by Stinson. Informally, a combinatorial AONT is an array with the unbiased requirements and its security properties in general depend on the prior probability distribution on the inputs \( s \)-tuples. Recently, it was shown by Esfahani and Stinson that a combinatorial AONT has perfect security provided that all the inputs \( s \)-tuples are equiprobable, and has weak security provided that all the inputs \( s \)-tuples are with non-zero probability. This paper aims to explore on the gap between perfect security and weak security for combinatorial \((t, s, v)\)-AONTs. Concretely, we consider the typical scenario that all the \( s \) inputs take values independently (but not necessarily identically) and quantify the information \( H(X|Y) \) about any \( t \) inputs \( X \) that is not revealed by any \( s-t \) outputs \( Y \).

The concept of an all-or-nothing transform (AONT) was introduced by Rivest [14], as a strongly non-separable mode of operation, that is a preprocessing step prior to encryption such that missing any cipher-block prevents the attacker from obtaining information about the message-blocks. The original motivation behind AONTs was to impede brute-force attacks on block ciphers when the key length cannot be increased [14]. Since then, numerous applications and extensions of AONTs have been studied and introduced within different context, e.g., cryptography, information security, and combinatorics [1], [2], [4], [6], [7], [13], [15]. Informally, an AONT is an unkeyed, invertible transformation which maps a sequence of inputs \((x_1, x_2, \ldots, x_s)\) to a sequence of outputs \((y_1, y_2, \ldots, y_s)\) with the following properties:

1. Given all \((y_1, y_2, \ldots, y_s)\), it is easy to compute \((x_1, x_2, \ldots, x_s)\); and
2. If any one of the \( y_j \) is missing, then it is computationally infeasible to obtain any information about any \( x_i \).

In contrast to the above computationally secure AONTs, Stinson [16] introduced the unconditionally secure AONT, which later was extended to the general scenario [5], [8] where more than one \( y_j \) could be missing. Here we recap the definition of unconditionally secure AONTs in terms of the entropy function \( H(\cdot) \) in [5].

**Definition 1:** Let \( X_1, \ldots, X_s \) and \( Y_1, \ldots, Y_s \) be input and output random variables respectively, which take values from the finite set \( \Gamma \) of size \( v \). These \( 2s \) random variables define a \((t, s, v)\)-AONT provided that the following conditions are satisfied:

1. \( H(Y_1, \ldots, Y_s | X_1, \ldots, X_s) = 0 \);
2. \( H(X_1, \ldots, X_s | Y_1, \ldots, Y_s) = 0 \);
3. For all \( \mathcal{X} \subseteq \{X_1, \ldots, X_s\} \) with \( |\mathcal{X}| = t \), and for all \( \mathcal{Y} \subseteq \{Y_1, \ldots, Y_s\} \) with \( |\mathcal{Y}| = s-t \), it holds that
   \[ H(\mathcal{X} | \mathcal{Y}) = H(\mathcal{X}). \]

Note that the items 1) and 2) in the above definition imply a one-to-one correspondence between inputs \( X_1, \ldots, X_s \) and outputs \( Y_1, \ldots, Y_s \). The item 3) guarantees the security property that no information about any \( t \) inputs can be learned from any \( s-t \) outputs, termed as the **perfect security** [10].

**A. Combinatorial AONTs**

In the meanwhile, the notion of combinatorial all-or-nothing transforms was proposed [5], [16]. We first recall some preliminary definitions. An \((N, K, v)\)-array \( A \) is an \( N \) by \( K \) array, whose entries are chosen from an alphabet \( \Gamma \) of order \( v \). Let \( I \subseteq [K] = \{1, 2, \ldots, K\} \), and \( A_I \) denote the array obtained from \( A \) by deleting all the columns indexed by \( c \in [K] \setminus I \).


---

1We remark that the entropy-based perfect security \( H(X|Y) = H(X) \) straightforwardly results the statistical distance \( SD(P_X | Y = y, P_X) = 0 \).

Indeed, \( H(X|Y) = H(X) \iff X \text{ and } Y \text{ are independent} \iff P(x|y) = P(x) \text{ holds for all } x \text{ and } y \iff \text{the statistical distance between } P_X | Y = y \text{ and } P_X \text{, for all } y, \text{ is } 0. \)
We say that $A$ is unbiased with respect to $I$ if the rows of $A_I$ contain every $|I|$-tuple in $\Gamma^{|I|}$ exactly $\frac{N}{\mu^{|I|}}$ times. Based on the unbiased property, the combinatorial AONT is defined as follows.

**Definition 2:** A combinatorial $(t, s, v)$-AONT is a $(v^s, 2s, v)$-array $A$ with columns labeled $1, \ldots, 2s$, which is unbiased with respect to the following subsets of columns:

1. $\{1, \ldots, s\}$
2. $\{s+1, \ldots, 2s\}$
3. $I \cup J$, for all $I \subseteq \{1, \ldots, s\}$ with $|I| = t$ and all $J \subseteq \{s+1, \ldots, 2s\}$ with $|J| = s - t$.

The existence and constructions of combinatorial AONTs have been extensively investigated, see [5], [7]–[9], [16], [18], [19] for example.

To see the connections between the AONT (based on $X_1, \ldots, X_s, Y_1, \ldots, Y_s$) in Definition 1 and the combinatorial AONT (based on array $A$) in Definition 2, we can think of the first $s$ columns of $A$ as the inputs $X_1, \ldots, X_s$ and the last $s$ columns of $A$ as the outputs $Y_1, \ldots, Y_s$. (In what follows, we also refer to the $i$th column of $A$ as the input $X_i$ and the $(s+i)$th column of $A$ as the output $Y_i$ for $1 \leq i \leq s$ when it is clear from the context.) Accordingly, the properties 1 and 2 in Definition 1 are equivalent to the properties (1) and (2) in Definition 2 in the sense that each of them implies a one-to-one correspondence between inputs and outputs. However, in contrast to the perfect security in the property 3 of Definition 1, the item (3) in Definition 2 only ensures that knowledge of any $s - t$ outputs does not rule out any possible values for any $t$ inputs, which is called the weak security in [10].

It is readily seen that there is a gap between the perfect security and the weak security. Indeed, as pointed out in [10], the entropy-based Definition 1 involves the “security” of an AONT, while the combinatorial AONT in Definition 2 is just a certain mathematical structure and its security properties in general depend on the underlying (prior) probability distribution on the possible inputs. Also notice that the input probability distributions together with the combinatorial AONT array induce a probability distribution on the outputs. Naturally, the following problem arises.

**Problem 3:** What are the security properties of combinatorial AONTs for given (prior) probability distributions on the inputs?

Esfahani and Stinson [10] provided answers to Problem 3 in the following cases.

**Theorem 4:** [10, Theorems 2.1 and 2.3]:

1. A combinatorial $(t, s, v)$-AONT has weak security provided that all the input $s$-tuples have non-zero probability.
2. A combinatorial $(t, s, v)$-AONT has perfect security if and only if all the input $s$-tuples are equally probable, i.e., each with probability $1/v^s$.

In addition to the aforementioned, the security properties of combinatorial AONTs are generally unknown. In this paper, we aim to explore on the gap between perfect security and weak security, as well as to provide more answers to Problem 3. Concretely, we consider the typical scenario that all the $s$ inputs take values independently (but not necessarily identically) and quantify $H(\mathcal{X} | \mathcal{Y}^o)$, i.e., the amount of information about any $t$ inputs $\mathcal{X}$ that is not revealed by any $s - t$ outputs $\mathcal{Y}$. In particular, we establish the general lower and upper bounds on $H(\mathcal{X} | \mathcal{Y}^o)$ for combinatorial $(t, s, v)$-AONTs (see Theorem 10) by making use of information-theoretic methods. Among others, in contrast to the perfect security with $H(\mathcal{X} | \mathcal{Y}^o) = H(\mathcal{X})$ and the weak security with $0 < H(\mathcal{X} | \mathcal{Y}^o) \leq H(\mathcal{X})$, we find an interesting phenomenon that for any $t$ inputs $\mathcal{X}$ and any $s - t$ outputs $\mathcal{Y}$, it holds that

$$H(\mathcal{X} | \mathcal{Y}^o) \leq \min_{\mathcal{X}'} H(\mathcal{X'})$$

where the min is taken over all the $t$ inputs set $\mathcal{X}' \subseteq \{X_1, \ldots, X_s\}$. It is also proven that this upper bound can be attained when there are at most $t$ non-uniform inputs (see Theorem 14). Some further discussions on the security properties of combinatorial $(t, s, v)$-AONTs in the case when $s$ inputs have partial dependency are also provided. Parts of the results on (symmetric) AONTs are referred to [12] as well.

**B. Asymmetric AONTs**

On the other hand, very recently, Esfahani and Stinson [11] generalized the $(t, s, v)$-AONT to the asymmetric $(t_i, t_o, s, v)$-AONT by replacing the parameter $t$ by two parameters $t_i$ and $t_o$ such that $t_i \leq t_o$, which has practical applications in the secure distributed storage system [7], [13] as well. Here we formulate the unconditionally secure asymmetric AONT in terms of entropy functions.

**Definition 5:** Let $X_1, \ldots, X_s$ and $Y_1, \ldots, Y_s$ be input and output random variables respectively, which take values from the finite set $\Gamma$ of size $v$. Let $1 \leq t_i \leq t_o \leq s$. These $2s$ random variables define an asymmetric $(t_i, t_o, s, v)$-AONT provided that the following conditions are satisfied:

1. $H(Y_1, \ldots, Y_s | X_1, \ldots, X_s) = 0$.
2. $H(X_1, \ldots, X_s | Y_1, \ldots, Y_s) = 0$.
3. For all $\mathcal{X} \subseteq \{X_1, \ldots, X_s\}$ with $|\mathcal{X}| = t_i$, and for all $\mathcal{Y} \subseteq \{Y_1, \ldots, Y_s\}$ with $|\mathcal{Y}| = s - t_o$, it holds that

$$H(\mathcal{X} | \mathcal{Y}^o) = H(\mathcal{X}).$$

The item 3) of the above definition implies the perfect security property of an asymmetric $(t_i, t_o, s, v)$-AONT, i.e., knowledge of all but $t_o$ outputs leaves any $t_i$ inputs completely undetermined. Note that when $t_i = t_o$, the asymmetric $(t_i, t_o, s, v)$-AONT reduces to the (symmetric) $(t, s, v)$-AONT. Hence the asymmetric $(t_i, t_o, s, v)$-AONT is mainly considered for the case when $t_i \leq t_o$.

A formulation of the combinatorial asymmetric AONT is presented in [11].

**Definition 6:** A combinatorial asymmetric $(t_i, t_o, s, v)$-AONT is a $(v^s, 2s, v)$-array $A$ with columns labeled $1, \ldots, 2s$, which is unbiased with respect to the following subsets of columns:

1. $\{1, \ldots, s\}$
2. $\{s+1, \ldots, 2s\}$
3. $I \cup J$, for all $I \subseteq \{1, \ldots, s\}$ with $|I| = t_i$ and all $J \subseteq \{s+1, \ldots, 2s\}$ with $|J| = s - t_o$. 

By Definitions 2 and 6, it is readily seen that a combinatorial \((t, s, v)\)-AONT is a combinatorial asymmetric \((t_1, t, s, v)\)-AONT for any \(1 \leq t_i \leq t\). The weak security property of a combinatorial asymmetric \((t_1, t_0, s, v)\)-AONT specifies that knowledge of any \(s-t_0\) outputs does not rule out any possible values for any \(t_i\) inputs. Notice that when \(t_1 < t_0\), the weak security property of a combinatorial asymmetric \((t_1, t_0, s, v)\)-AONT does not necessarily require that all the input \(s\)-tuples are with positive probability. Inspired by this, Esfahani and Stinson [11] relaxed the requirements of unbiased property on combinatorial asymmetric AONTs to the covering property, and then introduced the notion of combinatorial asymmetric weak-AONTs.

Let \(A\) be an \((N, K, v)\)-array over the alphabet \(\Gamma\) of order \(v\). Let \(I \subseteq [K] = \{1, 2, \ldots, K\}\) and \(A_I\) be the array obtained from \(A\) by deleting all the columns indexed by \(c \in [K] \setminus I\). We say that \(A\) is covering with respect to \(I\) if the rows of \(A_I\) contain every \(|I|\)-tuple in \(\Gamma^{|I|}\) at least once.

**Definition 7:** A combinatorial asymmetric \((t_1, t_0, s, v)\)-weak-AONT is a \((v^s, 2s, v)\)-array \(A\) with columns labeled \(1, \ldots, 2s\), which is covering with respect to the following subsets of columns:

1. \(\{1, \ldots, s\}\);
2. \(\{s + 1, \ldots, 2s\}\);
3. \(I \cup J\), for all \(I \subseteq \{1, \ldots, s\}\) with \(|I| = t_1\) and all \(J \subseteq \{s + 1, \ldots, 2s\}\) with \(|J| = s - t_0\).

It is easily seen that a combinatorial asymmetric \((t_1, t_0, s, v)\)-AONT is a combinatorial asymmetric \((t_1, t_0, s, v)\)-weak-AONT, but not vice versa. The existence and constructions of combinatorial asymmetric (weak)-AONTs have been studied in [7], [11]. Notice that the combinatorial asymmetric AONT and weak-AONT are mathematical structures. In terms of their security, the following problem appears.

**Problem 8:** What are the security properties of combinatorial asymmetric \((t_1, t_0, s, v)\)-(weak)-AONTs for given (prior) probability distributions on the inputs?

The following answers to Problem 8 can be found in [11].

**Theorem 9:** [11, Theorem 2.3]:

1. A combinatorial asymmetric \((t_1, t_0, s, v)\)-(weak)-AONT has weak security if all the input \(s\)-tuples have positive probability.
2. A combinatorial asymmetric \((t_1, t_0, s, v)\)-AONT has perfect security if every input \(s\)-tuple occurs with the same probability \(1/v^s\).

Except for the above-mentioned, the security properties of combinatorial asymmetric AONTs are unknown in general. This paper is devoted to exploring their security properties which are sandwiched between the known perfect security and weak security, as well as to providing answers to Problem 8. Again, we consider the typical scenario that all the \(s\) inputs take values independently but not necessarily identically, and quantify the amount of information \(H(\mathcal{X}|\mathcal{Y})\) about any \(t\) inputs \(\mathcal{X}\) that is not learned by any \(s-t\) outputs \(\mathcal{Y}\). By generalizing the discussions on combinatorial AONTs, we establish general lower and upper bounds on \(H(\mathcal{X}|\mathcal{Y})\) for combinatorial asymmetric AONTs (see Theorem 20). It is also shown that the established bounds could be attained in certain cases. In addition, some discussions on the differences of security properties between combinatorial asymmetric AONTs and combinatorial (symmetric) AONTs are presented as well.

The remainder of this paper is organized as follows. Section II establishes general lower and upper bounds for combinatorial AONTs, and shows that the derived bounds could be achieved in certain cases. Section III and Section IV discuss the security properties for combinatorial asymmetric AONTs and combinatorial asymmetric weak-AONTs respectively. Finally Section V concludes this paper.

## II. AONTs With Independent Inputs

In this section, we first prove the general lower and upper bounds on \(H(\mathcal{X}|\mathcal{Y})\) for combinatorial AONTs with independent inputs. Then we show that the derived bounds can be achieved in certain cases.

### A. General Bounds for Combinatorial AONTs

In this subsection, we establish the following theorem.

**Theorem 10:** Let array \(A \in \Gamma^{v^s} \times 2s\) be a combinatorial \((t, s, v)\)-AONT whose columns are with respect to random variables \(X_1, \ldots, X_s, Y_1, \ldots, Y_s\). Let \(P_1, \ldots, P_s\) be the corresponding probability distributions of \(X_1, \ldots, X_s\), which are mutually independent \(^2\) and take values from \(\Gamma\). Then for any input sets \(\mathcal{X}, \mathcal{X}' \subseteq \{X_1, \ldots, X_s\}\) such that \(|\mathcal{X}| = |\mathcal{X}'| = t\), and any \(s-t\) outputs \(\mathcal{Y} \subseteq \{Y_1, \ldots, Y_s\}\) such that \(|\mathcal{Y}| = s-t\), the followings hold.

1. \(H(\mathcal{X}|\mathcal{Y}) = H(\mathcal{X}'|\mathcal{Y}).\) (3)

2. \(H(\mathcal{X}|\mathcal{Y}) \geq \max \left\{0, \sum_{i \in [s]} H(X_i) - (s-t) \log(v)\right\}.\) (4)

3. \(H(\mathcal{X}|\mathcal{Y}) \leq \min_{\mathcal{X}' \subseteq \{X_1, \ldots, X_s\}} H(\mathcal{X}') = \min_{\mathcal{X}' \subseteq \{X_1, \ldots, X_s\}} \sum_{i \in I} H(X_i) \leq H(\mathcal{X}).\) (5)

In order to prove Theorem 10, we first show the following lemma.

**Lemma 11:** Under the assumption of Theorem 10, for any \(t\) inputs \(\mathcal{X} \subseteq \{X_1, \ldots, X_s\}\) such that \(|\mathcal{X}| = t\) and any \(s-t\) outputs \(\mathcal{Y} \subseteq \{Y_1, \ldots, Y_s\}\) such that \(|\mathcal{Y}| = s-t\), we have

\[
H(\mathcal{X}|\mathcal{Y}) = \sum_{i \in [s]} H(X_i) - H(\mathcal{Y}).\] (6)

\(^2\)For a collection of random variables, the random variables are called mutually independent if each random variable is independent of any combination of other random variables in the collection.
Proof: Let $\mathcal{X} = \{X_1, \ldots, X_s\} \setminus \mathcal{Y}$. Then by the definition, we have

\[
H(\mathcal{X} \mid \mathcal{Y}) = H(\mathcal{X}, \mathcal{Y}) - H(\mathcal{Y}) = \sum_{u \in \Gamma^t} \sum_{v \in \Gamma^{s-t}} \Pr[\mathcal{X} = u, \mathcal{Y} = v] \log \frac{1}{\Pr[\mathcal{X} = u, \mathcal{Y} = v]} - H(\mathcal{Y})
\]

where (7) follows from the unbiased property of the combinatorial $(t, s, v)$-AONT, i.e., each pair of $\mathcal{X} = u, \mathcal{Y} = v$ uniquely determines a $u' \in \Gamma^{s-t}$ such that $\mathcal{X} = u'$; and (8) follows from the assumption that all $X_i$ are mutually independent. This proves the lemma.

Indeed, by the assumption of combinatorial $(t, s, v)$-AONT, we have

\[
H(\mathcal{Y}) = \sum_{v \in \Gamma^{s-t}} \Pr[\mathcal{Y} = v] \log \frac{1}{\Pr[\mathcal{Y} = v]}
\]

where (11) follows from the unbiased property of the combinatorial $(t, s, v)$-AONT, i.e., each pair of $\mathcal{X} = u, \mathcal{Y} = v$ uniquely determines a $u' \in \Gamma^{s-t}$ such that $\mathcal{X} = u'$; and (12) follows from the mutual independence among $X_1, \ldots, X_s$; (13) follows from Lemma 12 with $\sum_{u \in \Gamma^t} \Pr[\mathcal{X}\mathcal{Y} = u, \mathcal{X}\mathcal{Y} = u'] = 1$ and $\Pr[\mathcal{X}\mathcal{Y} = u, \mathcal{X}\mathcal{Y} = u'] \geq 0$; (14) follows by switching the two sums on $v$ and $u'$ which is doable due to their independence; and (15) follows from the assumption of combinatorial $(t, s, v)$-AONT and its unbiased property. Thus the claim holds.

Combining Lemma 11 with (10), we obtain

\[
H(\mathcal{X} \mid \mathcal{Y}) = \sum_{i \in [s]} H(X_i) - H(\mathcal{Y}) \leq \sum_{i \in [s]} H(X_i) - H(\mathcal{X}\mathcal{Y})
\]
TABLE I
A COMBINATORIAL (1, 2,3)-AONT OVER THE ALPHABET {a, b, c}

| \(X_1\) | \(X_2\) | \(Y_1\) | \(Y_2\) |
|-------|-------|-------|-------|
| a     | a     | a     | a     |
| a     | b     | b     | b     |
| a     | c     | b     | b     |
| b     | a     | b     | b     |
| b     | b     | a     | c     |
| b     | c     | a     | c     |
| c     | a     | c     | c     |
| c     | b     | a     | b     |
| c     | c     | a     | b     |

\[
= \sum_{i \in [s]} H(X_i) - \sum_{X \in X_{\text{max}}} H(X)
= \min_{i \in [s]} \sum_{i \in I} H(X_i).
\]

This completes the proof. \(\square\)

Regarding the item 1) of Theorem 10, we remark that for any distinct output sets \(Y, Y' \subseteq \{Y_1, \ldots, Y_s\}\) such that \(Y \neq Y'\) and \(|Y| = |Y'| = s - t\), the relation \(H(X|Y) = H(X'|Y')\) does not hold in general, even for the case when \(X = X'\) (see Example 13). However the equality \(H(X|Y) = H(X'|Y')\) always holds in the case when at most \(t\) inputs are with non-uniform distributions (see Section II-B).

Also we would remark that the upper bound in Theorem 10 is tight in the sense that it can be achieved in certain cases (see Section II-B). In contrast, it is also worth noting that in general \(H(X|Y)\) depends on the input distributions and the upper bound in Theorem 10 might not always be attained, see Example 13 below considering the case when more than \(t\) inputs are with non-uniform distributions.

Example 13: Consider the combinatorial (1, 2,3)-AONT over the alphabet \(\Gamma = \{a, b, c\}\) shown in Table I as in [10].

Suppose that

\[
\Pr[X_1 = a] = \frac{1}{12}, \quad \Pr[X_1 = b] = \frac{1}{8}, \quad \Pr[X_1 = c] = \frac{5}{8},
\]

\[
\Pr[X_2 = a] = \frac{1}{3}, \quad \Pr[X_2 = b] = \frac{1}{6}, \quad \Pr[X_2 = c] = \frac{1}{2}.
\]

Plugging into Table I gives

\[
\Pr[Y_1 = a] = \frac{5}{12}, \quad \Pr[Y_1 = b] = \frac{13}{48}, \quad \Pr[Y_1 = c] = \frac{5}{16},
\]

\[
\Pr[Y_2 = a] = \frac{1}{4}, \quad \Pr[Y_2 = b] = \frac{19}{48}, \quad \Pr[Y_2 = c] = \frac{17}{48}.
\]

Then by the definition, it is easy to calculate

\[
H(X_1) = 1.298795, \quad H(X_2) = 1.459148, \quad H(Y_1) = 1.561053, \quad H(Y_2) = 1.559607.
\]

According to Lemma 11 and (3), we obtain

\[
H(X_1|Y_1) = H(X_2|Y_1) = H(X_1) + H(X_2) - H(Y_1) = 1.196889 < \min\{H(X_1), H(X_2)\},
\]

\[
H(X_1|Y_2) = H(X_2|Y_2) = H(X_1) + H(X_2) - H(Y_2) = 1.198335 < \min\{H(X_1), H(X_2)\},
\]

while it is easy to see \(H(X_1|Y_1) \neq H(X_1|Y_2)\) and \(H(X_2|Y_1) \neq H(X_2|Y_2)\).

B. AONTs With at Most \(t\) Non-Uniform Inputs

In this subsection, we consider the situation where at most \(t\) inputs are with non-uniform distributions. It is shown that the bounds in Theorem 10 turn to be tight in this case.

Theorem 14: Under the assumption of Theorem 10, if at most \(t\) of \(P_1, \ldots, P_s\) are non-uniform, then for any \(t\) inputs \(X \subseteq \{X_1, \ldots, X_s\}\) and any \(s - t\) outputs \(Y \subseteq \{Y_1, \ldots, Y_s\}\) such that \(|Y| = s - t\), we have

\[
H(X|Y) = \min_{|X'| = t} H(X^\prime) = \min_{|I| = t} \sum_{i \in I} H(X_i) \leq H(X).
\]

(16)

In other words, if \(P_1, \ldots, P_s\), where \(1 \leq r \leq t\), are non-uniform, and all the others \(P_1, \ldots, P_s\) are uniform, then

\[
H(Y|X) = H(X_{i_1}) + \cdots + H(X_{i_t}) + (t - r) \log(v). \quad (17)
\]

Proof: The conclusion follows from the lower and upper bounds in Theorem 10 in which all the inputs in \(X_{\text{max}}\) are with the uniform distribution. \(\square\)

Notice that the above theorem assumes the mutual independence among all inputs \(X_1, \ldots, X_s\). In the following, we show that the conclusion as in Theorem 14 also holds even for the case that a local dependence among at most \(t\) inputs exists. Precisely, we have the following theorem.

Theorem 15: Let array \(A \in \Gamma^{s \times 2s}\) be a combinatorial \((t, s, v)\)-AONT whose columns are with respect to random variables \(X_1, \ldots, X_s, Y_1, \ldots, Y_s\). If there are at most \(t\) inputs \(X_0, X_1, \ldots, X_s\) are mutually independent 3 and with the uniform distribution, then for any \(t\) inputs \(X \subseteq \{X_1, \ldots, X_s\}\) such that \(|X| = t\) and any \(s - t\) outputs \(Y \subseteq \{Y_1, \ldots, Y_s\}\) such that \(|Y| = s - t\), we have

\[
H(Y|X) = \min_{|X'| = t} H(X^\prime). \quad (18)
\]

Proof: First, similar to Lemma 11, for any \(t\) inputs \(X \subseteq \{X_1, \ldots, X_s\}\) such that \(|X| = t\) and any \(s - t\) outputs \(Y \subseteq \{Y_1, \ldots, Y_s\}\) such that \(|Y| = s - t\), we have

\[
H(Y|X) = H(X_1, \ldots, X_s) - H(Y). \quad (19)
\]

According to the assumption we can assume that \(X_U \subseteq \{X_1, \ldots, X_s\}\) such that \(|X_U| = s - t\) be a set of \(s - t\) mutually independent inputs with uniform probability distribution. Let \(X_U = \{X_1, \ldots, X_s\}\). Clearly \(|X_U| = t\) and \(X_0 \subseteq X_U\).

We first claim that in this setting for any \(s - t\) outputs \(Y \subseteq \{Y_1, \ldots, Y_s\}\) such that \(|Y| = s - t\),

\[
H(Y) = H(X_U) = (s - t) \log(v). \quad (20)
\]

Indeed, the above (20) can be verified by following the same line as the argument for (10), in which the equality in (13) is achieved according to Lemma 12 with \(\Pr[X_{\text{max}} = \mathbf{u}] = \Pr[X_U = \mathbf{u}] = \frac{1}{v^{|\mathbf{u}|}}\) for any \(\mathbf{u} \in \Gamma^{s - t}\). Here we would provide an alternative (and simpler) proof for (20) as below by directly showing that the probability distribution on \(Y\) is uniform.

3It also implicitly assumes that any input in \(X_0\) is independent of any combination of other inputs in \(\{X_1, \ldots, X_s\}\).
It suffices to prove that \( \Pr[\mathcal{Y} = v] = \frac{1}{v^{s-t}} \) for any \( v \in \Gamma^{s-t} \), i.e., outputs \( \mathcal{Y} \) take values on all \((s-t)\)-tuples with equal probability. Indeed,

\[
\Pr[\mathcal{Y} = v] = \sum_{u' \in \Gamma^t} \Pr[\mathcal{X}_U = u, \mathcal{X}_U' = u']
\]

(21)

\[
= \sum_{u' \in \Gamma^t} \Pr[\mathcal{X}_U = u] \cdot \Pr[\mathcal{X}_U' = u']
\]

(22)

\[
= \frac{1}{v^{s-t}} \cdot \sum_{u' \in \Gamma^t} \Pr[\mathcal{X}_U = u']
\]

(23)

Plugging into Table I gives

\[
\Pr[Y_1 = a] = \frac{1}{3}, \quad \Pr[Y_1 = b] = \frac{1}{3}, \quad \Pr[Y_1 = c] = \frac{1}{3},
\]

\[
\Pr[Y_2 = a] = \frac{1}{3}, \quad \Pr[Y_2 = b] = \frac{1}{3}, \quad \Pr[Y_2 = c] = \frac{1}{3}.
\]

Then by the definition, it is easy to calculate

\[
H(X_1) = 1.584963, \quad H(X_2) = 1.459148,
\]

\[
H(Y_1) = 1.584963, \quad H(Y_2) = 1.584963.
\]

III. ASYMMETRIC AONTs WITH INDEPENDENT INPUTS

In this section we investigate the security properties of combinatorial asymmetric AONTs with independent inputs. In particular, we establish the following theorem.

**Theorem 20:** Let array \( A \in \Gamma^{t_x} \times \Gamma^{2s} \) be a combinatorial asymmetric \((t_i, t_o, s, v)\)-aONT whose columns are with respect to random variables \( X_1, \ldots, X_s, Y_1, \ldots, Y_s \). Let \( P_1, \ldots, P_s \) be the corresponding probability distributions of \( X_1, \ldots, X_s \), which are mutually independent and take values from \( \Gamma \). Then for any \( t_i \) inputs \( \mathcal{X} \subseteq \{X_1, \ldots, X_s\} \) such that \( |\mathcal{X}| = t_i \), and any \( s - t_o \) outputs \( \mathcal{Y} \subseteq \{Y_1, \ldots, Y_s\} \) such that \( |\mathcal{Y}| = s - t_o \), the followings hold.

1) \[
H(\mathcal{X}|\mathcal{Y}) \geq \max \left\{ 0, \sum_{i=1}^{s} H(X_i) - (s - t_i) \log(v) \right\}.
\]

(24)

2) \[
H(\mathcal{X}|\mathcal{Y}) \leq \min \left\{ H(\mathcal{X}), \frac{\min_{\mathcal{I} \subseteq \{i_1, \ldots, i_s\}} \sum_{i \in \mathcal{I}} H(X_i) + (t_o - t_i) \log(v)}{s}, \right\}
\]

\[
\frac{\min_{\mathcal{I} \subseteq \{i_1, \ldots, i_s\}} \sum_{i \in \mathcal{I}} H(X_i) + s \cdot \log(v) - \sum_{i=1}^{s} H(X_i)}{s}.
\]

(25)

We would remark that Theorem 20 for combinatorial asymmetric \((t_i, t_o, s, v)\)-AONTs can be seen as a generalization of Theorem 10 for combinatorial \((t, s, v)\)-AONTs in the sense that the upper and lower bounds in Theorem 20 could deduce the bounds in Theorem 10 by letting \( t_i = t_o = t \). However, when \( t_i < t_o \), the property 1) of Theorem 10 does not hold in general for combinatorial asymmetric \((t_i, t_o, s, v)\)-AONTs (see Example 23). Furthermore, in contrast to Theorem 10, the quantification of \( H(\mathcal{X}|\mathcal{Y}) \) for combinatorial asymmetric \((t_i, t_o, s, v)\)-AONTs cannot be upper bounded by \( \min_{\mathcal{X}' \subseteq \mathcal{X}} H(\mathcal{X}') \) in general (see Example 23).
A. A General Lemma

In order to prove Theorem 20, we first prove the following lemma.

Lemma 21: Under the assumption of Theorem 20, for any $t_i$ inputs $\mathcal{X} \subseteq \{X_1, \ldots, X_s\}$ such that $|\mathcal{X}| = t_i$ and any $s - t_o$ outputs $\mathcal{Y} \subseteq \{Y_1, \ldots, Y_s\}$ such that $|\mathcal{Y}| = s - t_o$, we have

$$H(\mathcal{X}|\mathcal{Y}) \geq \sum_{i \in [s]} H(X_i) - (t_o - t_i) \log(v) - H(\mathcal{Y}),$$

(26)

$$H(\mathcal{X}|\mathcal{Y}) \leq \min \left\{ \sum_{i \in [s]} H(X_i) - H(\mathcal{Y}),
\left( s + t_i - t_o \right) \log(v) - H(\mathcal{Y}) \right\}.$$  

(27)

The following log-sum inequality will be exploited.

Lemma 22 [3]: For positive numbers $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$,

$$\sum_{i=1}^{n} a_i \log \frac{a_i}{b_i} \geq \left( \sum_{i=1}^{n} a_i \right) \log \left( \sum_{i=1}^{n} \frac{a_i}{b_i} \right)$$

with equality if and only if \( \frac{a_i}{b_i} = \text{constant}. \)

Proof of Lemma 21: Let \( \mathcal{X} = \{X_1, \ldots, X_s\} \setminus \mathcal{Y} \). For any $u \in \Gamma^{t_i}$, $v \in \Gamma^{s-t_o}$, denote

$$\mathcal{U}_{u,v} := \{ u' \in \Gamma^{s-t_i} : \exists \ a \ row \ in \ array \ A \ such \ that \ A = u, \mathcal{X} = u', \mathcal{Y} = v \}.$$  

(28)

According to the unbiased property of array $A$, it holds that

$$|\mathcal{U}_{u,v}| = v^{t_o-t_i}.$$  

(29)

By the definition, we have

$$H(\mathcal{X}, \mathcal{Y}) = - \sum_{u \in \Gamma^{t_i}, v \in \Gamma^{s-t_o}} \Pr[\mathcal{X} = u, \mathcal{Y} = v] \log \left( \Pr[\mathcal{X} = u, \mathcal{Y} = v] \right)$$

$$= - \sum_{u \in \Gamma^{t_i}, v \in \Gamma^{s-t_o}} \left( \sum_{u' \in \mathcal{U}_{u,v}} \Pr[\mathcal{X} = u, \mathcal{X} = u'] \cdot \log \left( \sum_{u' \in \mathcal{U}_{u,v}} \Pr[\mathcal{X} = u, \mathcal{X} = u'] \right) \right)$$

$$= - \sum_{u \in \Gamma^{t_i}, v \in \Gamma^{s-t_o}} \left( \sum_{u' \in \mathcal{U}_{u,v}} \Pr[\mathcal{X} = u] \cdot \Pr[\mathcal{X} = u'] \cdot \log \left( \sum_{u' \in \mathcal{U}_{u,v}} \Pr[\mathcal{X} = u] \cdot \Pr[\mathcal{X} = u'] \right) \right)$$

$$= - \sum_{u \in \Gamma^{t_i}, v \in \Gamma^{s-t_o}} \Pr[\mathcal{X} = u] \left( \sum_{u' \in \mathcal{U}_{u,v}} \Pr[\mathcal{X} = u'] \right) \cdot \log \left( \sum_{u' \in \mathcal{U}_{u,v}} \Pr[\mathcal{X} = u'] \right)$$

(30)

$$- \sum_{u \in \Gamma^{t_i}} \Pr[\mathcal{X} = u] \log \left( \Pr[\mathcal{X} = u] \right)$$

$$- \sum_{u \in \Gamma^{t_i}, v \in \Gamma^{s-t_o}} \Pr[\mathcal{X} = u] \log \left( \Pr[\mathcal{X} = u] \right) \cdot \sum_{u' \in \mathcal{U}_{u,v}} \Pr[\mathcal{X} = u']$$

(31)

$$\frac{1}{|\mathcal{U}_{u,v}|} \Pr[\mathcal{X} = u'] \log \left( \sum_{u' \in \mathcal{U}_{u,v}} \frac{1}{|\mathcal{U}_{u,v}|} \Pr[\mathcal{X} = u'] \right).$$

Notice that the formula (31) can be written as

$$- \sum_{u \in \Gamma^{t_i}, v \in \Gamma^{s-t_o}} \Pr[\mathcal{X} = u] \cdot |\mathcal{U}_{u,v}| \cdot g_{u,v}$$

$$- \sum_{u \in \Gamma^{t_i}, v \in \Gamma^{s-t_o}} \Pr[\mathcal{X} = u] \left( \sum_{u' \in \mathcal{U}_{u,v}} \Pr[\mathcal{X} = u'] \log \left( \Pr[\mathcal{X} = u'] \right) \right) \log \left( \Pr[\mathcal{X} = u] \right)$$

$$\ge - \sum_{u \in \Gamma^{t_i}, v \in \Gamma^{s-t_o}} \Pr[\mathcal{X} = u] \cdot |\mathcal{U}_{u,v}| \cdot g_{u,v}$$

$$\cdot \left( \sum_{u' \in \mathcal{U}_{u,v}} \frac{1}{|\mathcal{U}_{u,v}|} \Pr[\mathcal{X} = u'] \log \left( \Pr[\mathcal{X} = u'] \right) \right)$$

(33)

$$- (t_0 - t_i) \log(v) \sum_{u \in \Gamma^{t_i}, u' \in \Gamma^{s-t_i}} \Pr[\mathcal{X} = u] \Pr[\mathcal{X} = u']$$

$$= - \sum_{u \in \Gamma^{t_i}} \Pr[\mathcal{X} = u] \sum_{u' \in \mathcal{U}_{u,v}} \Pr[\mathcal{X} = u'] \log \left( \Pr[\mathcal{X} = u'] \right)$$

(34)

$$- (t_0 - t_i) \log(v)$$

(35)

$$= H(\mathcal{X}) - (t_0 - t_i) \log(v)$$

(36)

where (33) follows from Lemma 12 with $\sum_{u' \in \mathcal{U}_{u,v}} \frac{1}{|\mathcal{U}_{u,v}|} = 1$ and $\Pr[\mathcal{X} = u'] \geq 0$; (34) and (35) follow from (28) and (29). Also the formula (32) can be expressed as

$$\sum_{u \in \Gamma^{t_i}} \Pr[\mathcal{X} = u] \log \left( \Pr[\mathcal{X} = u] \right) \left( \sum_{u' \in \Gamma^{s-t_i}} \Pr[\mathcal{X} = u'] \right)$$

$$= H(\mathcal{X}).$$

(37)

Plugging (36) and (37) into (31) and (32) yields

$$H(\mathcal{X}, \mathcal{Y}) \geq H(\mathcal{X}) - (t_0 - t_i) \log(v) + H(\mathcal{X})$$

$$= \sum_{i \in [s]} H(X_i) - (t_o - t_i) \log(v)$$

and hence

$$H(\mathcal{X}|\mathcal{Y}) = H(\mathcal{X}, \mathcal{Y}) - H(\mathcal{Y})$$

$$\geq \sum_{i \in [s]} H(X_i) - (t_0 - t_i) \log(v) - H(\mathcal{Y}),$$

implying the lower bound (26).
Next we verify the upper bound (27). First, by (30) and the monotonically increasing property of $\log_2(\cdot)$ function,

\[
H(X, Y) \leq - \sum_{u \in \Gamma_t} \sum_{u' \in \mathcal{U}_{u,v}} \Pr[\mathcal{X} = u, \mathcal{X} = u'] \cdot \log \left( \Pr[\mathcal{X} = u, \mathcal{X} = u'] \right)
= - \sum_{u \in \Gamma_t} \Pr[\mathcal{X} = u, \mathcal{X} = u'] \log \left( \Pr[\mathcal{X} = u, \mathcal{X} = u'] \right) = H(X, \mathcal{X}),
\]

implying

\[
H(X|Y) \leq H(X, \mathcal{X}) - H(Y) = \sum_{i \in [s]} H(X_i) - H(Y). \tag{38}
\]

Also, from (30) together with Lemma 22 we have

\[
H(X, \mathcal{Y}) \leq \sum_{u \in \Gamma_t} \sum_{u' \in \mathcal{U}_{u,v}} \Pr[\mathcal{X} = u, \mathcal{X} = u'] \cdot \log \frac{\sum_{u \in \Gamma_t} \sum_{u' \in \mathcal{U}_{u,v}} 1}{\sum_{u \in \Gamma_t}} \Pr[\mathcal{X} = u, \mathcal{X} = u'] = (s + t_i - t_o) \log(v)\\
\]

which implies

\[
H(X|\mathcal{Y}) \leq (s + t_i - t_o) \log(v) - H(Y). \tag{39}
\]

Combining (38) and (39) gives the upper bound. This completes the proof.

It is worth noting that when $t_i = t_o$, the above Lemma 21 implies Lemma 11. In other words, the lower and upper bounds in Lemma 21 turn out to be tight in certain cases.

**B. Proof of Theorem 20**

**Proof of Theorem 20:**

1) According to Lemma 21, we have

\[
H(X|\mathcal{Y}) \geq \sum_{i \in [s]} H(X_i) - (t_o - t_i) \log(v) - H(Y)
\geq \sum_{i \in [s]} H(X_i) - (t_o - t_i) \log(v) - (s - t_i) \log(v)
= \sum_{i \in [s]} H(X_i) - (s - t_i) \log(v)
\]

where the second inequality follows from the fact $H(Y, Y') \leq H(Y) + H(Y')$ and $H(Y) \leq \log(v)$ for any output $Y$. Together with the non-negativity of entropy, the lower bound (24) follows.

2) Recall that $X_1, \ldots, X_s$ are mutually independent. Let $\mathcal{X}_{\text{max}} \subseteq \{X_1, \ldots, X_s\}$ such that $|\mathcal{X}_{\text{max}}| = s - t_i$ denote a collection of input random variables according to the largest $s - t_i$ entropy values among $H(X_1), \ldots, H(X_s)$. Denote $\mathcal{X}_{\text{max}} = \{X_1, \ldots, X_s\} \setminus \mathcal{X}_{\text{max}}$. Clearly, $|\mathcal{X}_{\text{max}}| = t_i$. In order to derive an upper bound on $H(X|\mathcal{Y})$ based on Lemma 21, we need to evaluate on $H(Y)$. For notation convenience, we denote

\[
g_{\text{max}} = \left( \sum_{u \in \mathcal{U}_{u,v}} \frac{1}{|\mathcal{U}_{u,v}|} \Pr[\mathcal{X}_{\text{max}} = u] \right) \cdot \log \left( \sum_{u \in \mathcal{U}_{u,v}} \frac{1}{|\mathcal{U}_{u,v}|} \Pr[\mathcal{X}_{\text{max}} = u] \right).
\]

And we have

\[
H(Y) = - \sum_{v \in \Gamma_t} \Pr[\mathcal{Y} = v] \log \left( \Pr[\mathcal{Y} = v] \right)\\
= - \sum_{v \in \Gamma_t} \left( \sum_{u \in \Gamma_t} \sum_{u' \in \mathcal{U}_{u,v}} \Pr[\mathcal{X}_{\text{max}} = u, \mathcal{X}_{\text{max}} = u'] \cdot \log \left( \sum_{u \in \Gamma_t} \sum_{u' \in \mathcal{U}_{u,v}} \Pr[\mathcal{X}_{\text{max}} = u, \mathcal{X}_{\text{max}} = u'] \right) \right)\tag{40}
\]

\[
\geq - \sum_{v \in \Gamma_t} \left( \sum_{u \in \Gamma_t} \Pr[\mathcal{X}_{\text{max}} = u] \sum_{u' \in \mathcal{U}_{u,v}} \Pr[\mathcal{X}_{\text{max}} = u'] \cdot \log |\mathcal{U}_{u,v}| \left( \sum_{u \in \Gamma_t} \sum_{u' \in \mathcal{U}_{u,v}} \Pr[\mathcal{X}_{\text{max}} = u] \sum_{u' \in \mathcal{U}_{u,v}} \Pr[\mathcal{X}_{\text{max}} = u'] \right) \right)\tag{41}
\]

where (40) follows from the assumption of combinatorial asymmetric $(t_i, t_o, s, v)$-AONT and (28); (41) follows from Lemma 12 with $\sum_{u \in \Gamma_t} \Pr[\mathcal{X}_{\text{max}} = u] = 1$ and
Together with Table II, we obtain which gives

\[ H(X'_i) = \frac{1}{6}, \quad H(X'_j) = \frac{1}{3}, \quad H(X'_k) = \frac{1}{2}. \]

which yields

\[ H(X'_1) = 1.459148, \quad H(X'_2) = 1.500000, \]
\[ H(X'_3) = 1.156780. \]

Together with Table II, we obtain

\begin{align*}
H(X_1|Y_1) & = 1.067794, \quad H(X_1|Y_2) = 1.459148, \\
H(X_1|Y_3) & = 1.381719, \quad H(X_2|Y_1) = 1.500000, \\
H(X_2|Y_2) & = 1.098856, \quad H(X_2|Y_3) = 1.381719, \\
H(X_3|Y_1) & = 1.067794, \quad H(X_3|Y_2) = 1.098856, \\
H(X_3|Y_3) & = 1.156780
\end{align*}

from which it is easy to see \( H(X_i|Y_j) \neq H(X_i|Y_{j'}) \) for all \( i, j, j' \in \{1, 2, 3\} \) with \( j \neq j' \). It is readily seen that

\[ H(X_1|Y_2) > H(X_3) = \min\{H(X_1), H(X_2), H(X_3)\}. \]

### IV. Asymmetric Weak-AONTs With Independent Inputs

This section discusses the security properties of combinatorial asymmetric weak-AONTs with independent inputs. We have the following theorem, which extends the discussions in the preceding Section III.

**Theorem 24:** Let array \( A \in \Gamma^{v^s \times 2s} \) be a combinatorial asymmetric \((t_i, t_o, s, v)\)-AONT whose columns are with respect to random variables \( X_1, \ldots, X_s, Y_1, \ldots, Y_s \). Let \( P_1, \ldots, P_s \) be the corresponding probability distributions of \( X_1, \ldots, X_s \), which are mutually independent and take values from \( \Gamma \). Then for any \( t_i \) inputs \( \mathcal{X} \subseteq \{X_1, \ldots, X_s\} \) such that \( |\mathcal{X}| = t_i \) and any \( s - t_o \) outputs \( \mathcal{Y} \subseteq \{Y_1, \ldots, Y_s\} \) such that \( |\mathcal{Y}| = s - t_o \), the followings hold.

1) \[ H(\mathcal{X}|\mathcal{Y}) \geq \max \left\{ 0, \sum_{j=1}^{s} H(X_j) - (s - t_o) \log(v) \right\} - \log \left( v^{s-t_i} - v^{s-t_o} + 1 \right). \] (44)

2) \[ H(\mathcal{X}|\mathcal{Y}) \leq \min \left\{ H(\mathcal{X}), \min_{|\mathcal{X}| = t_i} \sum_{j \in \mathcal{X}} H(X_j) + \log \left( v^{s-t_i} - v^{s-t_o} + 1 \right) \right\}. \] (45)

To prove Theorem 24, we will make use of the following lemma.

**Lemma 25:** Under the assumption of Theorem 24, for any \( t_i \) inputs \( \mathcal{X} \subseteq \{X_1, \ldots, X_s\} \) such that \( |\mathcal{X}| = t_i \) and any \( s - t_o \) outputs \( \mathcal{Y} \subseteq \{Y_1, \ldots, Y_s\} \) such that \( |\mathcal{Y}| = s - t_o \), we have

\[ \sum_{u \in \mathcal{U}} \Pr[X_{\text{max}} = u'] \geq 0; \] and (42) follows from Lemma 12 with

\[ \sum_{u \in \mathcal{U}} \frac{1}{|\mathcal{U}|} = 1 \text{ and } \Pr[X_{\text{max}} = u'] \geq 0. \]
TABLE III
A \((1, 2, 3, 2)\)-WEAK-AONT OVER THE ALPHABET \(\{a, b\}\)

| \(X_1\) | \(X_2\) | \(X_3\) | \(Y_1\) | \(Y_2\) | \(Y_3\) |
|---------|---------|---------|---------|---------|---------|
| a       | a       | a       | b       | a       | a       |
| a       | a       | b       | b       | b       | a       |
| a       | b       | a       | b       | a       | b       |
| a       | b       | b       | a       | a       | a       |
| b       | a       | a       | b       | b       | b       |
| b       | a       | b       | a       | b       | a       |
| b       | b       | a       | a       | b       | a       |
| b       | b       | b       | b       | b       | b       |

outputs \(\mathcal{Y} \subseteq \{Y_1, \ldots, Y_s\}\) such that \(|\mathcal{Y}| = s - t_o\), we have

\[
H(\mathcal{X}|\mathcal{Y}) \geq \sum_{j \in [s]} H(X_j) - \log (v^{s-t_i} - v^{s-t_o} + 1) - H(\mathcal{Y}) \tag{46}
\]

\[
H(\mathcal{X}|\mathcal{Y}) \leq \sum_{j \in [s]} H(X_j) - H(\mathcal{Y}). \tag{47}
\]

**Proof:** The proof can be done by following the same line as the arguments for Lemma 21. The only difference is as follows. Recall from (28) that

\[
\mathcal{U}'_{u,v} = \{u' \in \Gamma^{s-t_i} : \exists \text{ a row in array } A \text{ such that } X = u, \bar{X} = u', Y = v\}
\]

for any \(u \in \Gamma^{t_i}, v \in \Gamma^{s-t_o}\), and it holds that \(|\mathcal{U}'_{u,v}| = v^{t_o-t_i}\) for a combinatorial asymmetric \((t_i, t_o, s, v)\)-AONT due to its unbiased property. However, for a combinatorial asymmetric \((t_i, t_o, s, v)\)-weak-AONT, we only have

\[
1 \leq |\mathcal{U}'_{u,v}| \leq v^{s-t_i} - v^{s-t_o} + 1 \tag{48}
\]

according to its covering property. Replacing the quantization on \(|\mathcal{U}'_{u,v}|\) in the proof of Lemma 21 by the above estimation (48), it is not hard to derive the inequalities (46) and (47), and hence the lemma follows.

**Proof of Theorem 24:** Based on Lemma 25, the proof follows the same line as the argument of Theorem 20 by modifying the quantization of \(|\mathcal{U}'_{u,v}|\) by the inequality (48).

We would remark that the bounds in Theorem 24 could be tight in special cases, say when \(t_i = t_o\) and all the inputs are with uniform distribution. However, it is not always tight, see Example 26 below. Also in contrast to Theorem 10, Example 26 shows that neither the relation \(H(\mathcal{X}|\mathcal{Y}) = H(\mathcal{X}'|\mathcal{Y}')\) nor \(H(\mathcal{X}|\mathcal{Y}) = H(\mathcal{X}'|\mathcal{Y}')\) holds in general for any distinct \(\mathcal{X}, \mathcal{X}'\) and any distinct \(\mathcal{Y}, \mathcal{Y}'\).

**Example 26:** Consider the \((1, 2, 3, 2)\)-weak-AONT over the alphabet \(\Gamma = \{a, b\}\) shown in Table III as in [11].

Suppose that

\[
\Pr[X_1 = a] = \frac{1}{4}, \quad \Pr[X_1 = b] = \frac{3}{4},
\]

\[
\Pr[X_2 = a] = \frac{1}{3}, \quad \Pr[X_2 = b] = \frac{2}{3},
\]

\[
\Pr[X_3 = a] = \frac{1}{2}, \quad \Pr[X_3 = b] = \frac{1}{2}.
\]

Plugging into Table III gives

\[
\Pr[Y_1 = a] = \frac{13}{24}, \quad \Pr[Y_1 = b] = \frac{11}{24},
\]

\[
\Pr[Y_2 = a] = \frac{11}{24}, \quad \Pr[Y_2 = b] = \frac{13}{24},
\]

\[
\Pr[Y_3 = a] = \frac{7}{24}, \quad \Pr[Y_3 = b] = \frac{17}{24}.
\]

Then by the definition, it is easy to calculate

\[
H(X_1) = 0.811278, \quad H(X_2) = 0.918296,
\]

\[
H(X_3) = 1.00000, \quad H(Y_1) = 0.994985,
\]

\[
H(Y_2) = 0.994985, \quad H(Y_3) = 0.870864.
\]

Furthermore

\[
H(X_1|Y_1) = 0.667521, \quad H(X_1|Y_2) = 0.667521,
\]

\[
H(X_1|Y_3) = 0.657504, \quad H(X_2|Y_1) = 0.740788,
\]

\[
H(X_2|Y_2) = 0.740788, \quad H(X_2|Y_3) = 0.727952,
\]

\[
H(X_3|Y_1) = 0.735665, \quad H(X_3|Y_2) = 0.735665,
\]

\[
H(X_3|Y_3) = 0.836044,
\]

from which it is easy to see

\[
H(X_1|Y_1) = H(X_1|Y_2) \neq H(X_1|Y_3),
\]

and \(H(X_1|Y_1) \neq H(X_2|Y_1)\).

**V. CONCLUSION**

In this paper, we initially investigated the security properties sandwiched between perfect security and weak security for combinatorial AONTs and combinatorial asymmetric AONTs in the scenarios that all the \(s\) inputs take values independently but not necessarily identically and the even less restrictive model allowing partial dependency. By using information-theoretic techniques, we established general lower and upper bounds on the amount of information \(H(\mathcal{X}|\mathcal{Y})\) about any \(t_i\) inputs \(\mathcal{X}\) that is not revealed by any \(s-t_o\) outputs \(\mathcal{Y}\). It is also proven that the derived bounds could be attained in certain cases. However the security properties of combinatorial (asymmetric) AONTs are still unknown for many non-independent and non-identical (prior) probability distributions on the inputs, which is indeed of interest and worth investigating in the future work. In addition, to investigate the information-theoretic security properties of linear AONTs [16], in which each of the outputs is a linear combination of inputs and could be computed efficiently, with some prior input distributions is an interesting direction as well.

**ACKNOWLEDGMENT**

The authors express their gratitude to the anonymous reviewers for their detailed and constructive comments which are very helpful to the improvement of the presentation of this paper, and to Prof. Amos Beimel, the associate editor, for his excellent editorial job. They would also like to thank Prof. Douglas R. Stinson for reading an early version of this manuscript.
REFERENCES

[1] V. Boyko, “On the security properties of OAEP as an all-or-nothing transform,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 1666, Berlin, Germany: Springer, 1999, pp. 503–518.

[2] R. Canetti, Y. Dodis, S. Halevi, E. Kushilevitz, and A. Sahai, "Exposure-resilient functions and all-or-nothing transforms," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 1807, Berlin, Germany: Springer, 2000, pp. 453–469.

[3] T. Cover and J. Thomas, Elements of Information Theory. Hoboken, NJ, USA: Wiley, 2006.

[4] A. Desai, “The security of all-or-nothing encryption: Protecting against exhaustive key search,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 1880. Berlin, Germany: Springer, 2000, pp. 359–375.

[5] P. D’Arco, N. Esfahani, and D. Stinson, “All or nothing at all,” Electron. J. Combinatorics, vol. 23, no. 4, pp. 31–36, 2016.

[6] Y. Dodis, A. Sahai, and A. Smith, “On perfect and adaptive security in exposure-resilient cryptography,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 2045. Berlin, Germany: Springer, 2001, pp. 301–324.

[7] N. Esfahani, “Generalizations of all-or-nothing transforms and their application in secure distributed storage,” Ph.D. thesis, Cheriton School of Computer Sci., Univ. Waterloo, Waterloo, ON, Canada, 2021.

[8] N. Esfahani, I. Goldberg, and D. Stinson, “Some results on the existence of t-all-or-nothing transforms over arbitrary alphabets,” IEEE Trans. Inf. Theory, vol. 64, no. 4, pp. 3136–3143, Dec. 2018.

[9] N. Esfahani and D. Stinson, “Computational results on invertible matrices with the maximum number of invertible 2 × 2 submatrices,” Australas. J. Combinatorics, vol. 69, no. 1, pp. 130–144, 2017.

[10] N. Esfahani and D. Stinson, “On security properties of all-or-nothing transforms,” Designs, Codes Cryptogr., vol. 89, no. 12, pp. 2857–2867, Dec. 2021.

[11] N. Esfahani and D. Stinson, “Asymmetric all-or-nothing transforms,” 2021, arXiv:2105.14988.

[12] Y. Gu, S. Akao, N. Esfahani, Y. Miao, and K. Sakurai, “On the security properties of combinatorial all-or-nothing transforms,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jun. 2022.

[13] G. O. Karame, C. Soriente, K. Lichota, and S. Capkun, “Securing cloud data under key exposure,” IEEE Trans. Cloud Comput., vol. 7, no. 3, pp. 838–849, Jul./Sep. 2019.

[14] R. Rivest, “All-or-nothing encryption and the package transform,” in Fast Software Encryption (Lecture Notes in Computer Science), vol. 1267. Berlin, Germany: Springer, 1997, pp. 210–218.

[15] K. Sakurai, T. Nishide, and A. Syalim, “Improved proxy re-encryption scheme for symmetric key cryptography,” in Proc. Int. Workshop Big Data Inf. Secur. (IWBIS), Sep. 2017, pp. 105–111.

[16] D. Stinson, “Something about all-or-nothing (transforms),” Designs, Codes Cryptogr., vol. 22, pp. 133–138, Mar. 2001.

[17] D. Stinson and M. Paterson, Cryptography: Theory and Practice. Boca Raton, FL, USA: CRC Press, 2018.

[18] X. Wang, J. Cui, and L. Ji, “Linear (2, p, p)-AONTs exist for all primes p,” Designs, Codes Cryptogr., vol. 87, no. 10, pp. 2185–2197, Oct. 2019.

[19] Y. Zhang, T. Zhang, X. Wang, and G. Ge, “Invertible binary matrices with maximum number of 2-by-2 invertible submatrices,” Discrete Math., vol. 340, pp. 201–208, Feb. 2017.

Yujié Gu (Member, IEEE) received the Ph.D. degree from the Graduate School of Systems and Information Engineering, University of Tsukuba, Japan, in 2018. From 2018 to 2020, she was a Post-Doctoral Fellow with the Department of Electrical Engineering-Systems, Tel Aviv University, Israel.

Sonata Akao received the B.S. degree from Kyushu University, Japan, in 2021, where he is currently pursuing the master’s degree with the Graduate School of Information Science and Electrical Engineering.

Navid Nasr Esfahani received the B.Sc. degree from the Isfahan University of Technology, Isfahan, Iran, the M.Sc. degree from the University of Manitoba, Winnipeg, MB, Canada, and the Ph.D. degree from the Cheriton School of Computer Science, University of Waterloo, Waterloo, ON, Canada, under the supervision of Prof. Stinson. He is currently a Post-Doctoral Fellow with the CrySP Laboratory, University of Waterloo. His research interests include combinatorics, cryptography, information theoretic security, and privacy.

Ying Miao received the D.Sci. degree in mathematics from Hiroshima University, Hiroshima, Japan, in 1997. From 1995 to 1997, he was a Research Fellow with the Japan Society for the Promotion of Science. During 1997–1998, he was a Post-Doctoral Fellow at the Department of Computer Science, Concordia University, Montreal, QC, Canada. In 1998, he joined the University of Tsukuba, Tsukuba, Ibaraki, Japan, where he is currently a Full Professor with the Faculty of Engineering, Information and Systems. His current research interests include combinatorics, coding theory, information security, and their interactions.

Kouichi Sakurai (Member, IEEE) received the B.S. degree in mathematics from the Faculty of Science, Kyushu University, in 1986, and the M.S. degree in applied science and the Ph.D. degree in engineering from the Faculty of Engineering, Kyushu University, in 1988 and 1993, respectively.

From 1988 to 1994, he was engaged in research and development on cryptography and information security at the Computer and Information Systems Laboratory, Mitsubishi Electric Corporation. Since 1994, he has been working as an Associate Professor with the Department of Computer Science, Kyushu University, where he became a Full Professor, in 2002. He is concurrently working with the Institute of Systems, Information Technologies and Nanotechnologies, as the Chief of the Information Security Laboratory, for promoting research co-operations among the industry, university, and government under the theme enhancing IT-security in social systems.