Bit Security as Cost to Observe Advantage: Towards the Definition from THE BOOK*

Keewoo Lee

Seoul National University, Seoul, Republic of Korea
activecondor@snu.ac.kr

Abstract. We revisit the question of what should be the definition of bit security, previously answered by Micciancio-Walter (Eurocrypt 2018) and Watanabe-Yasunaga (Asiacrypt 2021). Our new definition is simple, but (i) captures both search and decision primitives in a single framework like Micciancio-Walter, and (ii) has a firm operational meaning like Watanabe-Yasunaga. It also matches intuitive expectations and can be easily well-estimated in terms of Kullback-Leibler divergence. Along the way of defining bit security and justifying our definition, we raise undervalued concepts such as allowing aborts in security games, considering partial adversaries, and verifiability in security games.

Keywords: Bit security · Security definitions · Kullback-Leibler divergence.

1 Introduction

Bit security (a.k.a. security level) is a central concept in cryptography, which bridges asymptotic and concrete regimes. Bit security summarizes complex security descriptions of a concrete instantiation of a cryptographic scheme in a single number, being a simple enough measure for level of security. Whereas asymptotic approach does not provide any guidance on concrete parameter selection, bit security helps us to choose an appropriate set of parameters to guarantee a certain level of security when deploying cryptographic schemes.

Despite its importance, we still do not have a well-accepted formal definition of bit security. Nonetheless, when we say a scheme has λ-bit security, we roughly expect that it costs more than 2^λ resources to break the scheme[1] or the scheme is as secure as its idealized version with a λ-bit secret key.

Conventional Definition. For search primitives (e.g. one-way function, signature), it is common to define bit security as $\min \log(T/\varepsilon)$. Here, the minimum

* According to Aigner-Ziegler in their eminent book entitled *Proofs from THE BOOK* [AZ99]: "Paul Erdős liked to talk about The Book, in which God maintains the perfect proofs for mathematical theorems, following the dictum of G. H. Hardy that there is no permanent place for ugly mathematics."

[1] An ambiguity here is how we define the word *break*.

is taken over all possible attacks $\mathcal{A}$, T is the cost (e.g. runtime) of $\mathcal{A}$, and ε is success probability (or advantage) of $\mathcal{A}$. The definition captures the tradeoff between cost and success probability for an idealized search primitive with a λ-bit secret key. Two trivial extreme attacks are (i) brute-force search with $T = 2^\lambda$ and $\varepsilon = 1$ (ii) guessing at random with $T = 1$ and $\varepsilon = 1/2^\lambda$. Another logic behind here is that the definition is consistent with *probability amplification*. Running an adversary $\mathcal{A}$ (with cost T and advantage ε) for N times, we have an adversary with cost $N \cdot T$ and advantage $1 - (1-\varepsilon)^N \approx N \cdot \varepsilon$, which yields essentially the same bit security.

On the other hand, for decision primitives (e.g. pseudorandom number generator, encryption), cryptography literature quantify the advantage of an adversary as $\varepsilon = |2P - 1|$, where P is the success probability.[2] Defining bit security of decision primitives analogously as $\min \log(T/\varepsilon)$, where ε is now the distinguishing advantage, sounds quite reasonable. This is the definition used implicitly in a number of cryptography literature. However, this conventional definition led to the following paradoxical situations.

Paradox One: Linear Test against PRG. It is a folklore, which goes back at least to [AGHP90], that there is a non-uniform attack (linear tests) against pseudorandom number generators (PRG) with λ-bit seed, which achieves advantage $2^{-\lambda/2}$ in time $O(\lambda)$. Thus, according to the conventional definition of bit security, a PRG with λ-bit seed can guarantee no more than $\lambda/2$-bit security. This is contrary to our expectation that λ-bit security of a PRG reflects the security of the ideal PRG with λ-bit seed. We note that the situation is not solely due to non-uniformity.[3] Non-uniform attacks on one-way functions (OWFs) can be handled if we choose a different cost measure, unlike the case of PRGs.[4] To resolve the mismatch, one might want to define bit security of decision primitives as $\min \log(T/\varepsilon^2)$. We remark that this alternative definition was considered by a few previous works [GL89, HILL99], but received little attention.

Paradox Two: Approximate Samplers. When constructing cryptographic schemes (especially in lattice-based cryptography [Reg05, Pei16]), we often make use of certain distributions (e.g. discrete Gaussian). That is, sampling from a particular distribution is often an important part of executing cryptographic schemes. And their security proofs assume an ideal situation where we can sample the distributions exactly. However, in real implementations, we can only sample from an approximated distribution due to limited resources.

[2] In decision primitives, guessing at random already achieves attack probability of $1/2$.

[3] We inform that there is some arguments on whether (e.g. [KM13]) and how (e.g. [BL13]) non-uniform adversaries should be considered in cryptography.

[4] De-Trevisan-Tulsiani [DTT10] proved the following lower bounds in the generic oracle setting, where T is the runtime, S is the amount of advice, ε is the corresponding advantage, and λ is the length of input or seed: (i) for OWFs, $S \cdot T = \tilde{\Omega}(\varepsilon \cdot 2^\lambda)$, and (ii) for PRGs, $S \cdot T = \tilde{\Omega}(\varepsilon^2 \cdot 2^\lambda)$. Using $S \cdot T$ as the cost measure, non-uniform attacks on OWFs can be well-addressed. However, this is not the case for PRGs.

The question to be answered is how does these approximations affect the security of the schemes. In terms of statistical distance (a.k.a. total variation distance), the standard measure in cryptography, it is an easy fact that λ-bit precision is required to achieve λ-bit security. While this sounds quite natural already, ambitious researchers have proved that it is enough to achieve roughly $\lambda/2$-bit closeness with respect to other *nice* divergences (e.g. Rényi [PDG14, BLL+15], max-log [MW17]), yielding much better parameters for practical uses.

However, all mentioned results apply only to search primitives[5], and a corresponding result for decision primitives has eluded researchers. The paradox is that it is generally believed that the security of encryption schemes (decision primitives) is more robust against approximation errors than that of signature schemes (search primitives).[6]

Previous Approaches. Micciancio-Walter [MW18] pointed out the paradoxes, and provided a general formal definition of bit security; their definition resolves the paradoxes and captures both search and decision primitives in a single framework. The main point of Micciancio-Walter is to consider a general cryptographic game in which an adversary has to guess an n-bit string, and define a general advantage of an adversary that captures both search (for large n) and decision (for $n = 1$) games, building on concepts from information theory.[7] However, in the definition, they introduce a hypothetical random variable that lacks intuitive meaning without a satisfactory explanation. (Refer to the original paper or Appendix B.2 for details.)

Watanabe-Yasunaga [WY21] pointed out this weakness of Micciancio-Walter as a lack of *operational meaning*, and provided another definition as cost for winning certain games with high probability — which also resolves the paradoxes mentioned and has an operational meaning by nature. However, they defined the games *qualitatively* differently for search and decision primitives, losing generality that Micciancio-Walter sought. (Refer to the original paper or Appendix B.3 for details.)

1.1 Our Contributions

Our main result is a new definition of bit security (Definition 3.6). Our definition is so simple that it can be expressed in plain language: we define bit security as the cost to *observe* advantage of adversaries (with high probability). Our simple definition (i) captures both search and decision primitives in a single framework like Micciancio-Walter [MW18] and (ii) has a firm operational meaning like Watanabe-Yasunaga [WY21]. Of course, our definition also resolves

[5] We excluded [BLL+15], which also considers decision primitives, because the result requires decision problems to satisfy a specific property called *public sampleability*.

[6] See, e.g., Section 4 of [ADPS16].

[7] Another point — considering adversaries that may explicitly declare failure of the attack ($\perp$) — is discussed later in Section 4.4.

the paradoxes (Section 4.3 and 4.4), matching the intuitive expectations. Moreover, our bit security provides a simple and tight estimation of itself in terms of Kullback-Leibler divergence (Section 3.2), suggesting practical usability of our definition. Besides, we:

- define a general framework which captures essentially all security games (Definition 3.1).
- introduce the trick of allowing adversaries to abort (Definition 3.1), in order to make it easier to resolve Paradox One (Section 4.2 and 4.3). This modification was also used in [MW18], but we use it in a more crucial way. (See Section 4.4.)
- point out yet another paradox in previous definitions of bit security (including [MW18, WY21]) and explain how our definition go past this paradox (Section 4.1).
- raise undervalued concepts such as:
  - allowing aborts in security games (Definition 3.1 and Section 4.2),
  - considering partial adversaries (Definition 3.6 and Section 4.5),
  - and verifiability in security games (Section 4.1).

Main messages from our work are the followings.

- Cryptography literature somehow overlooked the concept of verifiability in security games, although it is a significant concept in security definitions.
- The quadratic gap in Paradox One, which is the starting point of [MW18, WY21] and our work, is not from difference in size but from difference in verifiability.
- Allowing adversaries to abort might enable more handy security arguments in some cases.

1.2 Organization

This paper is divided into two main parts. The more technical and formal part, definitions, is presented in Section 3, and the more conceptual and informal part, discussions, is presented in Section 4.

After a short introduction on our notations and terminologies (Section 2), our new definition of bit security as cost to observe advantage (Definition 3.6) is presented in Section 3.1. Along the way, we also define a general framework to abstract all security games (Definition 3.1) and extend the traditional definition of advantage into our framework which allows adversaries to abort (Definition 3.3 and 3.4). In Section 3.2, we prove that our bit security can be well-approximated in terms of Kullback-Leibler divergence (Corollary 3.1). This suggests practical usability of our definition of bit security.

In Section 4, various level of discussions are presented. In Section 4.1, we point out yet another paradox in previous definitions of bit security, including [MW18, WY21]. Then, we claim that the paradox arises because the cryptography community have overlooked the concept of *verifiability*, and explain how our

definition go past this paradox. In Section 4.2, we try to convey our intuition behind our definition of (generalized) advantage (Definition 3.4) and explain the utility of allowing adversaries to abort. In Section 4.3, we perform case studies on our definition of bit security in order to resolve the Paradox One presented in Section 1. In Section 4.4, we compare our definition of security game and bit security with those of Micciancio-Walter [MW18] and Watanabe-Yasunaga [WY21][8], and eventually resolve the Paradox Two (Section 1). In Section 4.5, our humble opinion on the practice of considering partial adversaries is presented. In Appendix A, some marginal discussions are noted.

2 Notations and Terminologies

We denote the logarithm to the base 2 by $\log(\cdot)$ and the one to the base e by $\ln(\cdot)$. We use standard arithmetic over extended non-negative real numbers $[0, \infty]$ (e.g. $\frac{a}{0} = \infty$ and $\frac{a}{\infty} = 0$ for $a \in (0, \infty)$), but with an additional rule $\frac{0}{0} = 0$. In particular, the conditional probability $\Pr[\ \emptyset \mid \emptyset\ ]$ is defined to be zero. We denote the Kullback-Leibler divergence between the Bernoulli distributions with parameters p and q as $D_{\mathrm{KL}}(p||q) = p \cdot \log \frac{p}{q} + (1-p) \cdot \log \frac{1-p}{1-q}$. We note that $D_{\mathrm{KL}}(p||1) = \infty$ in our convention. We do not strictly distinguish the terms *hardness* and *security*, and often use them interchangeably.

3 Definitions

3.1 Bit Security as Cost to Observe Advantage

We first formally define a generic framework to clarify the scope of our new definition of bit security. However, we believe our framework is abstract enough to capture every security definitions in the cryptography literature.

Definition 3.1 (Security Game). *A* security game $G = (X, A, R)$ *is played by an adversary* $\mathcal{A}$ *interacting with a challenger* X*. At the end of game,* $\mathcal{A}$ *outputs some value* $a \in A \cup \{\bot\}$*, where* $\bot$ *is a predefined symbol to indicate the abort.*[9] *The adversary* $\mathcal{A}$ *wins the game if* $(\mathtt{view}_X, a) \in R$*, where* $\mathtt{view}_X \in \{0,1\}^*$ *is the* view *of the game from the perspective of the challenger* X *and the* target relation $R \subset \{0,1\}^* \times A$ *is a binary relation. We call the game a* decision game *if* $|A| = 2$*, and a* search game *if* $|A| > 2$*.*

At first glance, it may not seem like much, but the role of $\bot$ is crucial in this paper. (See Section 4.2 and 4.4.) We acknowledge that considering $\bot$ is highly influenced by Micciancio-Walter [MW18].

Going back to the basics and in the spirit of Watanabe-Yasunaga [WY21], which defines bit security as cost for winning certain games with high probability, we define bit security as the following.

[8] For readers who are not familiar with the previous definitions of [MW18, WY21], we summarize their definitions and some results in Appendix B.

[9] That is, $\bot$ can never be in A.

Definition 3.2 (Bit Security). *For any security game G, we denote and define its* bit hardness *(with respect to error probability $0 < \delta < 1/2$) as the following, where $T_{\mathcal{A}}$ is the cost of the adversary $\mathcal{A}$.*[10]

$$BS^{\delta}(G) = \min_{\mathcal{A}} \{\log T_{\mathcal{A}} : \Pr[\mathcal{A} \textit{ wins } G] \geq 1 - \delta\}$$

The bit security *of a cryptographic scheme Π_G, whose security is defined by the game G, is defined as the bit hardness of G.*

We call this definition of bit security the *primary version* to distinguish it from a later definition (Definition 3.6). The definition is more or less an implementation of our intuition on bit security by formally defining what is to *break* a cryptographic scheme, in terms of winning the security game with high probability. We remark that the definition indeed has a firm operational meaning and is independent of types of security games (e.g. decision or search).

But, now what?

While the primary version of bit security (Definition 3.2) only considers *full* adversaries, all the controversies on the definitions of bit security are about *partial* adversaries. That is, the central question in the line of works is, for example, how should the existence of an adversary with small but non-negligible success probability affect bit security. (See Section 4.5 for discussions on considering partial adversaries.) In the rest of this paper, we convey our answer to the question by a new definition of bit security generalizing Definition 3.2. We begin by refining the traditional definition of *advantage* of an adversary into our framework (Definition 3.1).

Definition 3.3 (Normalized Success Probability). *Let G be a security game and $\mathcal{A}$ be an adversary against G. We denote and define the* normalized success probability *of $\mathcal{A}$ against G as the following.*

$$P_{\mathcal{A}}^{G} = \Pr\left[\ \mathcal{A} \textit{ wins } G \ \middle|\ \mathcal{A} \textit{ does not abort}\ \right]$$

We denote and define the output probability *of $\mathcal{A}$ against G as the following.*

$$\alpha_{\mathcal{A}}^{G} = \Pr\left[\ \mathcal{A} \textit{ does not abort}\ \right]$$

Definition 3.4 (Advantage). *Let G be a security game. An adversary $\mathcal{A}$ against G is called a* dummy *if the output of $\mathcal{A}$ is independent of any inputs during the game. We denote and define the* baseline probability *of G as the following.*

$$P_0^G = \max_{\mathcal{A}:\textit{dummy}} P_{\mathcal{A}}^{G}$$

We denote and define the advantage *of $\mathcal{A}$ against G as the following.*

$$\mathrm{adv}^{G}(\mathcal{A}) = \max\left\{P_{\mathcal{A}}^{G} - P_0^G,\ 0\ \right\}$$

[10] In this paper, we fix a cost function T which maps an adversary to a non-negative integer. We expect T to be linear under repetition, i.e. $T_{\mathcal{A}^N} = N \cdot T_{\mathcal{A}}$ where $\mathcal{A}^N$ denotes the N-repetition of $\mathcal{A}$. While our definition is still valid when T is not linear, this results the definition to have less operational meaning.

It is easy to see that our definition matches with the traditional definition of advantage, when $\mathcal{A}$ never aborts. Our contribution and possibly a controversial point here is how well we extended the traditional definition into our framework which allows to abort. For discussions on this issue, refer to Section 4.2.

Next, we define an event, which we call the *observation of advantage*. It tries to capture the situation where the adversary demonstrates its advantage *empirically*, i.e. $\mathcal{A}$ wins significantly many games when the security game is repeated several times. We believe this is a very natural concept to consider when a partial adversary is given.

Definition 3.5 (Observation of Advantage). *Let G be a security game, $\mathcal{A}$ be an adversary against G, and N be a positive integer. When G is repeated N times independently and $\mathcal{A}$ wins more than P_0^G fraction of non-aborted games, we say the advantage of $\mathcal{A}$ is* observed *in G^N. We denote the probability of observing advantage of $\mathcal{A}$ in G^N as $P_{obs}^G(\mathcal{A}, N)$. That is,*

$$P_{obs}^G(\mathcal{A}, N) = \Pr\left[\frac{\#\text{ of games } \mathcal{A} \text{ wins in } N\text{-repeated } Gs}{\#\text{ of games } \mathcal{A} \text{ does not abort in } N\text{-repeated } Gs} > P_0^G\right].$$

Now we are ready to define bit security against partial adversaries. Our definition tries to capture the cost to *experience* the advantage of an adversary with high probability, leveraging Definition 3.5.

Definition 3.6 (Bit Security against Partial Adversaries). *For any security game G, we denote and define its* bit hardness against partial adversaries *(with respect to error probability $0 < \delta < 1/2$) as the following, where $T_{\mathcal{A}}$ is the cost of the adversary $\mathcal{A}$.*

$$BS_{Part}^{\delta}(G) = \min_{\mathcal{A},N} \left\{\log\left(N \cdot T_{\mathcal{A}}\right) : P_{obs}^G(\mathcal{A}, N) \geq 1 - \delta\right\}$$

The bit security against partial adversaries *of a cryptographic scheme Π_G, whose security is defined by the game G, is defined as the bit hardness of G against partial adversaries.*

Again, we remark that the definition is independent of types of security games (e.g. decision or search). We believe the definition also has a very firm and natural operational meaning.

The following proposition and its proof assert that our definition of bit security against partial adversaries is indeed a generalization of the primary definition. Although the bit security of Definition 3.6 does not exactly match that of Definition 3.2 in general, we can say that it is a more conservative measure to use, at least.

Proposition 3.1. *For any security game G and error probability $0 < \delta < 1/2$, the following inequality holds.*

$$BS_{Part}^{\delta}(G) \leq BS^{\delta}(G)$$

Proof. Easily follows from the fact that $\Pr[\mathcal{A} \text{ wins } G] = P_{obs}^G(\mathcal{A}, 1)$. □

3.2 Bit Security in terms of KL Divergence

Even if we agree on the plausibility of Definition 3.6, there remains question on its practical usability. In this regard, we show that bit security against partial adversaries can be well-approximated in terms of Kullback-Leibler divergence (a.k.a. KL divergence, Rényi divergence of order one).

Proposition 3.2 (Estimation of Observation Probability). *Let G be a security game, $\mathcal{A}$ be an adversary against G, and N be a positive integer. Assume that $P_0^G < P_{\mathcal{A}}^G < 1$. Then, the probability of observing advantage of $\mathcal{A}$ in G^N satisfies the following approximate bounds, where $D = D_{\mathrm{KL}}(P_0^G || P_{\mathcal{A}}^G)$.*

$$\frac{e^{-\alpha_{\mathcal{A}}^G \cdot D \cdot N}}{\sqrt{8 \cdot \alpha_{\mathcal{A}}^G \cdot P_0^G(1-P_0^G) \cdot N}} \lessapprox 1 - P_{obs}^G(\mathcal{A}, N) \lessapprox \quad e^{-\alpha_{\mathcal{A}}^G \cdot D \cdot N}$$

Proof. These are straightforward applications of a standard concentration bound (a.k.a. tail bound), namely the Chernoff bound, and an *anti*-concentration bound for binomial distributions (See e.g. [Ash12]), after approximating the number of non-aborted games as $\alpha_{\mathcal{A}}^G \cdot N$. □

Corollary 3.1 (Estimation of Bit Security against Partial Adversaries). *For any security game G and $0 < \delta < 1/2$, bit hardness of G against partial adversaries with respect to error probability δ can be estimated as the following.*

$$BS_{Part}^{\delta}(G) \approx \min_{\mathcal{A}} \log\left(N_{\mathcal{A}}^{\delta} \cdot T_{\mathcal{A}}\right)$$

Here, $N_{\mathcal{A}}^{\delta}$ is defined as follows.

$$N_{\mathcal{A}}^{\delta} = \frac{1}{\alpha_{\mathcal{A}}^G} \cdot \max\left\{ \frac{\ln(1/\delta)}{D_{\mathrm{KL}}\left(P_0^G || P_{\mathcal{A}}^G\right)} \ , \quad 1 \right\}$$

Proof. From Proposition 3.2, we have that $N_{\mathcal{A}}^{\delta} \approx \min\left\{N : P_{obs}^G(\mathcal{A}, N) \geq 1-\delta\right\}$. Then, apply it to the following trivial reformulation of $BS_{Part}^{\delta}(G)$.

$$BS_{Part}^{\delta}(G) = \min_{\mathcal{A}} \log\left(T_{\mathcal{A}} \cdot \min\left\{N : P_{obs}^G(\mathcal{A}, N) \geq 1-\delta\right\}\right)$$

□

Inspired from Corollary 3.1, we suggest yet another definition of bit security, namely *KL-bit security*. We believe the definition of KL-bit security (i) is as general as possible (as it is independent of types of games), (ii) is practically useful (as it is easily computable and its dependency on error probability is dropped), and (iii) also well-reflects the reality of security level (as it is an approximate version of Definition 3.6 which has a very firm operational meaning).

Definition 3.7 (KL-Advantage). *For any security game G and adversary $\mathcal{A}$ against G, we denote and define the* KL-advantage *of $\mathcal{A}$ against G as the following.*

$$\mathrm{adv}^G_{\mathrm{KL}}(\mathcal{A}) = \alpha^G_{\mathcal{A}} \cdot \min\left\{ D_{\mathrm{KL}}\left(P^G_0 || P^G_{\mathcal{A}}\right),\ 1 \right\}$$

Definition 3.8 (KL-Bit Security). *For any security game G, we denote and define its* KL-bit hardness *as the following, where $T_{\mathcal{A}}$ denotes the cost of the adversary $\mathcal{A}$.*

$$BS_{\mathrm{KL}}(G) = \min_{\mathcal{A}} \log\left(\frac{T_{\mathcal{A}}}{\mathrm{adv}^G_{\mathrm{KL}}(\mathcal{A})}\right)$$

The KL-bit security *of a cryptographic scheme Π_G, whose security is defined by the game G, is defined as the KL-bit hardness of G.*

The following proposition asserts that our definition of KL-bit security is at least a conservative measure to use.

Proposition 3.3. *For any security game G and error probability $0 < \delta \leq 1/e$, the following (approximate) inequalities holds.*

$$BS_{\mathrm{KL}}(G) \lessapprox BS^{\delta}_{Part}(G) \leq BS^{\delta}(G)$$

Proof. A straightforward combination of Proposition 3.1 and Corollary 3.1. □

4 Discussions

4.1 Verifiability

Paradox Three: Uniform Random Adversaries. Consider a decision game, in which the answer is uniformly distributed, and a dummy adversary which outputs a uniform random answer. The advantage of this adversary (in the traditional sense) is defined to be zero, and it makes perfect sense. Now, let us consider a *search* game, in which the answer is again uniformly distributed over a finite set, and again an adversary which outputs a uniform random answer. According to the conventional definition of bit security as $\min \log(T/\varepsilon)$ (Section 1 and Definition B.1), surprisingly, this uniform random adversary is not a dummy anymore in the search game: existence of such uniform random adversary already implies a finite bit security. A philosophy behind this work is that we can interpret decision games as search games with extremely small answer space. If this is true, something strange is happening here.

Verifiability. Our claim is that the key to this paradox is the concept of *verifiability*. We call a security game *verifiable* if adversaries have the access to an oracle which *verifies* whether the input satisfies the target relation of the game and outputs the result[11] (or there is a trivial way for adversaries to verify by

[11] It is required that the target relation is independent of verification queries.

oneself with negligible costs). If not, we call the game *non-verifiable*. That is, a verifiable game is a security game where adversaries have *power* to recognize their success and failure.

Of course, for decision games, verifiability is not a meaningful concept, as all nontrivial decision game is non-verifiable. If a decision game is verifiable, an adversary can always win the game with only two verifications. On the other hand, for search games, both verifiable and non-verifiable games seem considerable.

Verifiability as a Gift: Paradox Three Resolved. However, the cryptography literature somehow overlooked the concept of verifiability, took verifiable search games for granted, and neglected non-verifiable search games. The conventional definition of bit security (Section 1) apparently demonstrates the situation: brute-force search and (linear) probability amplification, which are intuition behind the definition, are only possible when the security game is verifiable.

Our claim is that, instead of taking verifiability for granted, if we consider the verifiability as a *bonus*, then we can resolve the above paradox. More technically, we defined dummy adversaries (Definition 3.4) so that they cannot perform verifications (even in a verifiable game). Then an adversary who has an access to verification deserves to be said having non-zero advantage, resolving the paradox. Our work suggests that the classification of verifiable versus non-verifiable games is much more fundamental than that of search versus decision games. This will be further supported in the scene where the Paradox One (Section 1) is resolved (Section 4.3).

Verifiability in Previous Works. The situation of oversight is not so different in the previous works which provide new definitions of bit security [MW18, WY21]. In particular, they are not concerned much about non-verifiable search games. Watanabe-Yasunaga [WY21] implicitly presumed verifiability of search games in their definition of bit security (Appendix B.3) and wrote "By definition, the bit security of search primitives has a finite value ... In contrast to this fact, decision games can have infinite bit security. For example, since the one-time pad (OTP) has perfect secrecy, the bit security should be unbounded." However, this phrase is very mistaken, as we can also define a proper one-wayness game for OTP, which is unarguably expected to be an ∞-bit hard search game. Even though non-verifiable search games were *explicitly* considered in [MW18, Section 5.2], Micciancio-Walter do not seem to be aware of their significance in security definitions. According to their definition of advantage for search games, an adversary has zero advantage only if it always either aborts or outputs a wrong answer.

We remark that non-verifiable search games are not pathological counterexamples devised just to tackle existing definitions. These include not only security games for primitives with information theoretic security (e.g. one-wayness game for OTP) but also the computational Diffie-Hellman problem (CDH), in which verification corresponds to solving the decisional Diffie-Hellman problem.

4.2 Power to Say "I Don't Know (⊥)"

If we agree on the power of verifiability, the next step would be to quantitatively study the power. Our starting point is to ask: what is the most distinct feature a partial adversary of a verifiable game have? We claim that it is the power to verify its answer *just before* the submission. If its answer is correct, nothing special happens: the adversary will output its original answer. However, if it is wrong, the adversary will definitely do something.

Let us first consider the setting where aborts are *not* allowed. In this case, the adversary will output another random answer.[12] Then, the success probability will be slightly amplified, but the resulting output distribution has no significant structural difference from that of non-verifiable adversaries. This makes it hard to study verifiable adversaries apart from non-verifiable ones.

So we use a trick: we allow adversaries to abort (Definition 3.1). Notice that outputting another random answer is essentially a *dummy* action whose success probability is very close to the baseline probability. In this regard, it seems fair enough *to not take the aborted game into account* (Definition 3.3), in order to give appropriate favors to adversaries who admitted their ignorance instead of guessing at random. In this way, we can implement the power of verifiability into the power to say "I Don't Know (⊥)", which gives significant structural difference on output distributions of verifiable versus non-verifiable adversaries. (See Footnote 13.)

4.3 Paradox One Resolved

In order to investigate how our definition (Definition 3.6 and 3.8) resolves the Paradox One (Section 1), we examine the following two cases.

First Case: $P^G_{\mathcal{A}} = 1$. This case of adversaries are considered to capture the behavior of adversaries against verifiable (search) games. In this case, we have the following equalities.

$$\mathrm{adv}^G_{\mathrm{KL}}(\mathcal{A}) = \alpha^G_{\mathcal{A}} \cdot \min\left\{ D_{\mathrm{KL}}\Big(P^G_0 \,||\, 1\Big),\ 1 \right\} = \alpha^G_{\mathcal{A}}$$

If we admit that running verification before outputting an answer (and abort if it is not a valid answer) is the best strategy[13] for verifiable games, then we

[12] We believe this is the hidden intuition behind the definition of the hypothetical random variable of [MW18] (Definition B.4), which explains why their definition of bit security works so well for *verifiable* search games.

[13] This is almost equivalent to the assumption that the cost for verification is negligible, under our definition of advantage (Definition 3.3 and 3.4). This is the point where our introduction of abort (Definition 3.1) and definition of advantage take effect.

have the following equalities for a verifiable search game G.

$$\begin{aligned} BS_{\mathrm{KL}}(G) &= \min_{P_{\mathcal{A}}^G=1} \log\left(\frac{T_{\mathcal{A}}}{\mathrm{adv}_{\mathrm{KL}}^G(\mathcal{A})}\right) \\ &= \min_{P_{\mathcal{A}}^G=1} \log\left(\frac{T_{\mathcal{A}}}{\alpha_{\mathcal{A}}^G \cdot P_{\mathcal{A}}^G}\right) \end{aligned}$$

Notice that $\alpha_{\mathcal{A}}^G \cdot P_{\mathcal{A}}^G$ is the success probability in the traditional sense. Therefore, our KL-bit security is consistent with the conventional definition of bit security (Definition B.1), for verifiable search games.

Second Case: $P_0^G = 1/2$. This case of games includes *balanced* decision games, where the correct answer is uniformly distributed. In this case, we have the following (approximate) equalities, where the approximation comes from the Taylor expansion at $P_{\mathcal{A}}^G = 1/2$. Hence, the approximation holds only when $P_{\mathcal{A}}^G$ is close to $1/2$.

$$\begin{aligned} \mathrm{adv}_{\mathrm{KL}}^G(\mathcal{A}) &= \alpha_{\mathcal{A}}^G \cdot \min\left\{D_{\mathrm{KL}}\left(1/2||P_{\mathcal{A}}^G\right),\ 1\right\} \\ &= \alpha_{\mathcal{A}}^G \cdot \min\left\{\frac{1}{2}\log\left(\frac{1}{P_{\mathcal{A}}^G(1-P_{\mathcal{A}}^G)}\right) - 1,\ 1\right\} \\ &\approx \frac{2}{\ln(2)} \cdot \alpha_{\mathcal{A}}^G \left(P_{\mathcal{A}}^G - \frac{1}{2}\right)^2 \\ &= \frac{2}{\ln(2)} \cdot \alpha_{\mathcal{A}}^G \cdot \left(\mathrm{adv}^G(\mathcal{A})\right)^2 \end{aligned}$$

If we neglect the constant term and admit that, in (non-verifiable) decision games, aborting is not a good idea, then we have the following equalities for a balanced decision game G.

$$\begin{aligned} BS_{\mathrm{KL}}(G) &= \min_{\alpha_{\mathcal{A}}^G=1} \log\left(\frac{T_{\mathcal{A}}}{\mathrm{adv}_{\mathrm{KL}}^G(\mathcal{A})}\right) \\ &= \min_{\alpha_{\mathcal{A}}^G=1} \log\left(\frac{T_{\mathcal{A}}}{\left(\mathrm{adv}^G(\mathcal{A})\right)^2}\right) \end{aligned}$$

Notice that this is the alternative definition of bit security (Definition B.1) for decision primitives, which was suggested to avoid paradoxical situation of linear tests against PRG (Section 1). Therefore, our KL-bit security is consistent with the expectation of the community, for balanced decision games, resolving the Paradox One (Section 1).

Opinion. We remark that our definition is not consistent with the conventional (resp. alternative) definition for all search (resp. decision) games in general.

Namely, our definition differs from the conventional (resp. alternative) definition for non-verifiable search games (resp. *unbalanced* decision games, where the distribution of the correct answer is unbalanced). However, we do not think this is a drawback of our definition. Instead, we believe this indicates that the conventional definition and the alternative definition neglected non-verifiable search games and unbalanced decision games. (See also Section 4.1 for discussions on verifiability.)

4.4 Comparison with Previous Definitions

Definition of Security Game. The principal feature of Definition 3.1 is that it allows adversaries to *abort*. The idea of considering abort ($\perp$) is highly influenced by the previous definition of Micciancio-Walter [MW18], whereas Watanabe-Yasunaga [WY21] do not consider these aborts. However, we believe our work employs the concept of abort in a much more significant way than [MW18]. This is because Micciancio-Walter seem to be using this powerful concept only in relatively minor parts (e.g. tightness of security reductions) of the discourse. (See also Section 4.1 for their oversight on the concept of verifiability.) In particular, the quadratic gap between bit security of search and decision game, which is the main question of [MW18] and our work, is explained in terms of the *size of the secrets* and not by allowing aborts. On the other hand, allowing abort is crucial in our definitions and we explain the quadratic gap leveraging this concept of abort (See Section 4.3).

Aiming to be as abstract and general as possible, our definition of security games does not restrict anything (except the ability to abort), and target relations are defined as relations between the *view* of the challenger and the answer of the adversary. On the other hand, previous works [MW18, WY21] define security games to begin with the challenger choosing a *secret*, and define target relations as relations between this *secret* and the answer of the adversary. We regard this as an unnatural and restrictive formulation, since we often consider security games where the secret (answer) is chosen during the game, i.e. the target relation is affected by the queries of an adversary (e.g. IND-CPA game for public key encryption schemes, EUF-CMA game for signature schemes). That is, previous definitions do not capture even the IND-CPA game without modifications, while ours seem to capture all existing security definitions.

Another difference is that we classify decision versus search games according to the size of the answer space, whereas previous works classify according to the size of the secret space. We believe our criteria is closer to reality, although distinction between decision and search games is not crucial in our work.

Bit Security of [WY21]. Our definition of bit security against partial adversaries (Definition 3.6) is highly influenced by Watanabe-Yasunaga [WY21]. It is defined as cost for an event to happen with high probability, with firm operational meaning, as in Watanabe-Yasunaga.

The biggest difference between [WY21] and our work is *generality*. Although they defined bit security for both search and decision primitives as computational

cost for winning games with high probability, the designated games for search and decision primitives differs *qualitatively*. On the other hand, our definition has a simple and natural description which is totally independent of game types. Moreover, our definition has a tight approximation in terms of KL-divergence (Proposition 3.1), which is a single formula independent of game types. Oversight of [WY21] on non-verifiable search games (Section 4.1) may also be stated as an issue of generality.

Bit Security of [MW18]. Our work and Micciancio-Walter [MW18] both seek for generality, under the belief that, since a decision game can be understood as a search game with extremely small answer space, there must not be a binary distinction between decision and search games. The solution of Micciancio-Walter was to *devise* an advantage which interpolates two extreme cases of $n = 1$ for decision games and $n \gg 1$ for search games. On the other hand, our work shows that there is a binary distinction but this distinction, in fact, stems from verifiability and not from decision/search types (Section 4.3).

However, in the aspect of naturality and interpretability, Micciancio-Walter introduces a hypothetical random variable in the definition, which lacks intuitive meaning without a sufficient explanation. On the other hand, our definition is based on the simple and natural concept of *observing advantage* (Definition 3.5) which has firm operational meaning by nature. Nonetheless, it is very surprising that the resulting bit security from two different approaches of [MW18] and ours are exactly the same (Section 4.3 and Theorem B.1). We believe there are some hidden operational meaning behind the random variable (See Footnote 12).

Paradox Two Resolved. As we mentioned above, the resulting bit security from the definitions of Micciancio-Walter [MW18] and ours are the same, if we restrict our interest to verifiable search games and balanced decision games. Thus, all security reductions proved in [MW18] can trivially translated into our framework. In particular, we obtain a version of the theorem which resolved the Paradox Two (Section 1) in [MW18] for free, resolving the paradox also in our framework. For the sake of completeness, we state the theorem adapted to our results, without a proof. The theorem roughly says approximating employed distributions upto $\lambda/2$-bit closeness (with respect to a *nice* divergence) is enough for λ-bit security, also in the case of decision primitives.

Theorem 4.1 ([MW18, Theorem 8 (Adapted)]). *Let $G^{\mathcal{P}}$ be a* balanced *decision game G instantiated with black-box access to a probability ensemble $\mathcal{P}$, $G^{\mathcal{Q}}$ be the similar, and D be a c-efficient measure*[14] *for any $c \leq \frac{1}{4}$. If $G^{\mathcal{P}}$ is λ-bit hard and $D(\mathcal{P}, \mathcal{Q}) \leq 2^{-\lambda/2}$, then $G^{\mathcal{Q}}$ is $(\lambda - \alpha)$-bit hard, where α is a small constant.*

[14] For the definition, refer to [MW17] or [MW18].

4.5 Practical Reality of Partial Adversaries

A fundamental question one can ask is:

Do we really need to consider partial adversaries?

Our honest answer is "I Don't Know ($\perp$)".[15]

The NO-aspect of our opinion is that, in theory, we do not have to. Our primary definition of bit security (Definition 3.2), which considers only full adversaries, seems to be the most natural definition one can think of. The main point is that we cannot extend a partial adversary to a full adversary in a black-box manner, in most of the security games. This is because, in most security games, the challenger chooses the challenge only once and the target relation is affected by the queries of an adversary. That is, *resetting* the game and starting from the beginning is not allowed in security games, in general. These games include very basic examples of IND-CPA game for public key encryption schemes and EUF-CMA game for signature schemes. Moreover, this limited access to the challenger might be crucial in some applications.

The YES-aspect of our opinion is that, in practice, the community actually cares about partial adversaries. Many researchers consider existence of partial adversaries as a harm to security, and essentially the goal of prior works by Micciancio-Walter [MW18] and Watanabe-Yasunaga [WY21] was to well-quantify this harm. Moreover, this unlimited access to the challenger seems to be reasonable in many situations.

Resettable Game. A radical opinion of ours is that these two aspects might indicate that our theory does not reflect our practice sufficiently. In this regard, we cautiously suggest to use security notions defined in a *resettable* manner, generally, and use *non-resettable* security games only when the limited access to the challenger is crucial in the scenario.

Then, another natural question rises: what should be the winning criteria for resettable security games, where the adversary may reset the *inner* security game and output answers multiple times? Our claim is that the concept of *observation of advantage* (Definition 3.5) is the most natural criteria one can think of. In this aspect, our work can be also understood as a work aiming to answer the questions of (i) how should the security of resettable games be formally defined, and (ii) how does bit security of a resettable game relate to the bit security of its *inner* security game.

References

ADPS16. Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange—a new hope. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 327–343, 2016. 3

[15] Power to say "I Don't Know ($\perp$)" was already discussed in Section 4.2

AGHP90. N Alon, O Goldreich, J Hastad, and R Peralta. Simple construction of almost k-wise independent random variables. In *Proceedings of the 31st Annual Symposium on Foundations of Computer Science*, pages 544–553, 1990. 2

Ash12. Robert B Ash. *Information theory*. Courier Corporation, 2012. 8

AZ99. Martin Aigner and Günter M Ziegler. Proofs from the book. *Berlin. Germany*, 1999. 1

BL13. Daniel J Bernstein and Tanja Lange. Non-uniform cracks in the concrete: the power of free precomputation. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 321–340. Springer, 2013. 2, 17

BLL+15. Shi Bai, Adeline Langlois, Tancrède Lepoint, Damien Stehlé, and Ron Steinfeld. Improved security proofs in lattice-based cryptography: Using the rényi divergence rather than the statistical distance. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 3–24. Springer, 2015. 3

DTT10. Anindya De, Luca Trevisan, and Madhur Tulsiani. Time space tradeoffs for attacks against one-way functions and prgs. In *Annual Cryptology Conference*, pages 649–665. Springer, 2010. 2, 17

GL89. Oded Goldreich and Leonid A Levin. A hard-core predicate for all one-way functions. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 25–32, 1989. 2

Gol11. Oded Goldreich. In a world of p= bpp. In *Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation*, pages 191–232. Springer, 2011. 17

HILL99. Johan Håstad, Russell Impagliazzo, Leonid A Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999. 2

KM13. Neal Koblitz and Alfred Menezes. Another look at non-uniformity. *Groups-Complexity-Cryptology*, 5(2):117–139, 2013. 2, 17

MW17. Daniele Micciancio and Michael Walter. Gaussian sampling over the integers: Efficient, generic, constant-time. In *Annual International Cryptology Conference*, pages 455–485. Springer, 2017. 3, 14

MW18. Daniele Micciancio and Michael Walter. On the bit security of cryptographic primitives. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 3–28. Springer, 2018. 3, 4, 5, 10, 11, 13, 14, 15, 17, 18

PDG14. Thomas Pöppelmann, Léo Ducas, and Tim Güneysu. Enhanced lattice-based signatures on reconfigurable hardware. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 353–370. Springer, 2014. 3

Pei16. Chris Peikert. A decade of lattice cryptography. *Foundations and Trends® in Theoretical Computer Science*, 10(4):283–424, 2016. 2

Reg05. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, pages 84–93, 2005. 2

WY21. Shun Watanabe and Kenji Yasunaga. Bit security as computational cost for winning games with high probability. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 161–188. Springer, 2021. 3, 4, 5, 10, 13, 14, 15, 17, 19

A More Discussions

Cost Functions. There are controversies over which is the most proper measure of cost, especially in the non-uniform setting, e.g. [KM13, BL13]. This is indeed related to our work and is an interesting question to investigate. Nonetheless, we believe the issue is orthogonal to our work, as we are concerned with the question of defining security after a cost function is fixed. At least, the most commonly used cost functions (e.g. time complexity, circuit size [DTT10], $S \cdot T$ defined in Footnote 4) meet our expectation of being linear under repetition (Footnote 10).

Definition of Bit Security. Our definition of bit security (Definition 3.2) can be understood as a straightforward average-concrete-interactive-search analogue of the computational complexity class BPP. That is, whereas (♠) BPP consists of decision problems solvable by a probabilistic polynomial time algorithm with a worst-case error probability bounded away from $0 < \delta < 1/2$, (♣) the set of security games which are *not* λ-hard consists of decision and search games solvable by a probabilistic algorithm whose cost is less than 2^λ with an average-case error probability bounded away from $0 < \delta < 1/2$.

To the best of our knowledge, a work by Goldreich [Gol11] is the only work which attempts to define a natural search analogue of BPP. Unfortunately, our definition does not match the definition of [Gol11], which only considers *verifiable* search problems. This is to avoid pathological halting-problem-related search problems which can be solved by a probabilistic polynomial-time algorithm but cannot be solved by a deterministic algorithm regardless of running time. As such pathological examples do not appear in our concrete regime and there are natural search problems which are conjectured to be *non-verifiable* (e.g. CDH), we believe our definition is fine without the restriction to verifiable search problems.

B Previous Definitions

In this appendix, we summarize definitions and some results from previous works [MW18, WY21]. Some expressions are modified for sake of consistency.

B.1 Conventional and Alternative Definition

Definition B.1 (Conventional). *For any security game G, we denote and define its* conventional bit hardness *as the following, where $T_{\mathcal{A}}$ is the cost of the adversary $\mathcal{A}$. When G is a search game, $\varepsilon_{\mathcal{A}}$ is defined as success probability of $\mathcal{A}$. When G is a decision game, $\varepsilon_{\mathcal{A}}$ is defined as distinguishing advantage of $\mathcal{A}$.*

$$BS^{\delta}_{\mathrm{Conv}}(G) = \min_{\mathcal{A}} \log\left(T_{\mathcal{A}}/\varepsilon_{\mathcal{A}}\right)$$

Definition B.2 (Alternative). *For any security game G, we denote and define its* alternative bit hardness *as the following, where $T_{\mathcal{A}}$ is the cost of the*

adversary $\mathcal{A}$. Here, $\varepsilon'_{\mathcal{A}}$ is defined as $\varepsilon'_{\mathcal{A}} := \varepsilon_{\mathcal{A}}$ when G is a search game, and $\varepsilon'_{\mathcal{A}} := (\varepsilon_{\mathcal{A}})^2$ when G is a decision game.

$$BS^{\delta}_{\mathrm{Conv}}(G) = \min_{\mathcal{A}} \log\left(T_{\mathcal{A}}/\varepsilon'_{\mathcal{A}}\right)$$

B.2 Micciancio-Walter [MW18]

Definition B.3 ([MW18, Definition 5]). *An n-bit* security game *is played by an adversary $\mathcal{A}$ interacting with a challenger X. At the beginning of the game, the challenger chooses a secret x, represented by the random variable $X \in \{0,1\}^n$, from some distribution $\mathcal{D}_X$. At the end of the game, $\mathcal{A}$ outputs some value, which is represented by the random variable $\mathcal{A}$. The adversary $\mathcal{A}$ wins the game if it outputs a value a such that $(x,a) \in R$, where R is some relation. A may output a special symbol $\perp$ such that $R(x,\perp)$ and $\bar{R}(x,\perp)$ are both false.*

Definition B.4 ([MW18, Definition 7]). *For any security game G and adversary $\mathcal{A}$ against G, we denote and define the* MW-advantage *of $\mathcal{A}$ against G as the following.*

$$\mathrm{adv}^{G}_{\mathrm{MW}}(\mathcal{A}) = \frac{I(X;Y)}{H(X)}$$

Here, $I(\cdot;\cdot)$ is the mutual information, $H(\cdot)$ is the Shannon entropy, and $Y(X,\mathcal{A})$ is the random variable with marginal distributions $Y_{x,a} = \{Y|X=x,\mathcal{A}=a\}$ defined as

1. *$Y_{x,\perp} = \perp$, for all x.*
2. *$Y_{x,a} = x$ for all $(x,a) \in R$.*
3. *$Y_{x,a} = \{x' \leftarrow \mathcal{D}_X | x' \neq x\}$, for all $(x,a) \in \bar{R}$.*

Definition B.5 ([MW18, Definition 8]). *For any security game G, we denote and define its* MW-bit hardness *as the following, where $T_{\mathcal{A}}$ denotes the cost of the adversary $\mathcal{A}$.*

$$BS_{\mathrm{MW}}(G) = \min_{\mathcal{A}} \log\left(\frac{T_{\mathcal{A}}}{\mathrm{adv}^{G}_{\mathrm{MW}}(\mathcal{A})}\right).$$

Theorem B.1 ([MW18, Theorem 1]). *For any n-bit security game G with uniform secret distribution, let $\mathcal{A}$ be an adversary. Then,*

$$\mathrm{adv}^{G}_{\mathrm{MW}}(\mathcal{A}) = \alpha^{G}_{\mathcal{A}}\left(1 - \frac{(1-P^{G}_{\mathcal{A}})\log(2^n-1) + H(P^{G}_{\mathcal{A}})}{n}\right),$$

where $H(P)$ denotes the Shannon entropy of the Bernoulli distribution with parameter P. Note that for $n \gg 1$ we get $\mathrm{adv}_{\mathrm{MW}}(\mathcal{A}) \approx \alpha^{G}_{\mathcal{A}} P^{G}_{\mathcal{A}}$ and for $n = 1$ we get $\mathrm{adv}_{\mathrm{MW}}(\mathcal{A}) \approx \frac{2}{\ln(2)}\alpha^{G}_{\mathcal{A}}(P^{G}_{\mathcal{A}} - 1/2)^2$.

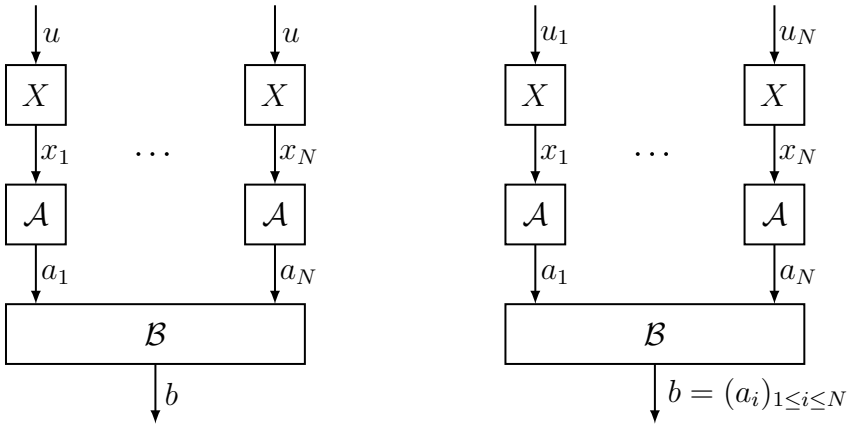
B.3 Watanabe-Yasunaga [WY21]

Definition B.6 ([WY21, Security Game]). *An n-bit security game $G = (X, R, O)$ consisting of an algorithm (challenger) X, a relation R, and an oracle O, is played by an adversary $\mathcal{A}$ given oracle access to O. At the beginning of the game, a secret $u \in \{0,1\}^n$ is chosen uniformly at random, and the challenge x is computed as $X(u)$. The goal of the adversary is to output a value a such that $(u, x, a) \in R$.*

Definition B.7 ([WY21, Outer Game]). *Let G be a security game and $\mathcal{A}$ be an adversary against G. When G is a decision game (i.e. 1-bit security game), the* outer game *of G with respect to $\mathcal{A}$ is played by an* outer *adversary $\mathcal{B}$, who wins the game if it outputs $u \in \{0,1\}$ given oracle access to $\mathcal{A}(X(u))$. See Figure 1a, where oracles in G are omitted. When G is a search game (i.e. n-bit security game with $n > 1$), the* outer game *of G with respect to $\mathcal{A}$ is played by an* outer *adversary $\mathcal{B}$, who invokes G several times and wins if there was any game $\mathcal{A}$ won. In other words, $\mathcal{B}$ has oracle access to $\mathcal{A}(X(u))$, where u is uniformly chosen from $\{0,1\}$ at the beginning of every queries. See Figure 1b, where oracles in G are omitted. The outer game of G with respect to $\mathcal{A}$ is denoted as $\hat{G}(\mathcal{A})$.*

Definition B.8 ([WY21, Bit Security]). *For any security game G, we denote and define its* WY-bit hardness *(with respect to error probability $0 < \delta < 1/2$) as the following, where $T_{\mathcal{A}}$ denotes the cost of the adversary $\mathcal{A}$ and $N_{\mathcal{B}}$ denotes the number of queries to $\mathcal{A}$ made by the outer adversary $\mathcal{B}$.*

$$BS^{\delta}_{WY}(G) = \min_{\mathcal{A},\mathcal{B}} \left\{ \log(N_{\mathcal{B}} \cdot T_{\mathcal{A}}) : \Pr[\mathcal{B} \text{ wins } \hat{G}(\mathcal{A})] \geq 1 - \delta \right\}$$



(a) Decision (b) Search

Fig. 1. Watanabe-Yasunaga