A limitation on security evaluation of cryptographic primitives with fixed keys

doi: 10.1002/sec.1457

SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2016; **9:**1663–1675
Published online 24 February 2016 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1457

SPECIAL ISSUE PAPER

A limitation on security evaluation of cryptographic primitives with fixed keys

Yutaka Kawai[1]*, Goichiro Hanaoka[2], Kazuo Ohta[3] and Noboru Kunihiro[4]

[1] Mitsubishi Electric. 5-1-1 Ofuna, Kamakukra, Kanagawa 247-8501, Japan
[2] National Institute of Advanced Industrial Science and Technology, Tsukuba, Japan
[3] The University of Electro-Communications, Chofu, Japan
[4] The University of Tokyo, Tokyo, Japan

ABSTRACT

In this paper, we discuss security of public-key cryptographic primitives in the case that the public key is fixed. In the standard argument, security of cryptographic primitives are evaluated by estimating the average probability of being successfully attacked where keys are treated as random variables. In contrast to this, in practice, a user is mostly interested in the security under his specific public key, which has been already fixed. However, it is obvious that such security cannot be mathematically guaranteed because for any given public key, there always potentially exists an adversary, which breaks its security. Therefore, the best what we can do is just to use a public key such that its effective adversary is not likely to be constructed in the real life and, thus, it is desired to provide a method for evaluating this possibility. The motivation of this work is to investigate (in)feasibility of predicting whether for a given fixed public key, its successful adversary will actually appear in the real life or not. As our main result, we prove that for any digital signature scheme or public key encryption scheme, it is impossible to reduce any fixed key adversary in any weaker security notion than the de facto ones (i.e., existential unforgery against adaptive chosen message attacks or indistinguishability against adaptive chosen ciphertext attacks) to fixed key adversaries in the de facto security notion in a black-box manner. This result means that, for example, for any digital signature scheme, impossibility of extracting the secret key from a fixed public key will never imply existential unforgery against chosen message attacks under the same key as long as we consider only black-box analysis.

KEYWORDS
public key encryption; digital signature; fixed key; impossibility; meta-reduction

***Correspondence**
Yutaka Kawai, Mitsubishi Electric. 5-1-1 Ofuna, Kamakukra, Kanagawa 247-8501, Japan.
E-mail: Kawai.Yutaka@da.mitsubishielectric.co.jp

1. INTRODUCTION

1.1. Background

A security notion of cryptographic primitives is addressed by a combination of an adversarial goal (GOAL) and an attack model (ATK), and we say that a cryptographic primitive satisfies GOAL-ATK security if no adversary can break it in the sense of GOAL even if access to oracles, which are determined by ATK, is allowed. In particular, for a digital signature schemes, existential unforgery (EuF)-chosen message attack (CMA) where EuF and CMA denote existential unforgery and adaptively chosen message attack, respectively, is considered as the standard security notion. As for a public key encryption scheme, indistinguishability (IND)-chosen ciphertext attack (CCA) where IND and CCA denote indistinguishability of plaintexts and adaptively chosen message attack, respectively, is the standard one. These two notions also imply universal composability [1,2], which guarantees that the security will not be degraded under concurrent use with other cryptographic primitives.

Indeed, so far, a number of digital signature and public key encryption schemes, which are *provably* EuF-CMA or IND-CCA secure, have been proposed where we say a cryptographic primitive is provably GOAL-ATK secure if existence of an adversary ,which breaks it with a non-negligible probability in the sense of GOAL-ATK, always implies existence of an algorithm, which solves the underlying mathematically hard problem, which is assumed

intractable. Here, we also notice that the probability of succeeding in the attack is estimated by taking the public key as a random variable, and therefore, even provable EuF-CMA security does not immediately imply that the digital signature scheme securely works under a specific public key. However, in the real world usage, once a key of a digital signature scheme is generated, a user keeps to use this fixed public key for a relatively long-time period. Thus, from the viewpoint of users, security under their fixed keys is more important than the average security over all keys. Actually, there is no contradiction even if in a provably EuF-CMA secure digital signature scheme, there exists a public key whose corresponding secret key is easily recovered. In an asymptotic sense, the probability of picking such a weak key is negligible if the scheme is provably EuF-CMA secure. However, in practical systems, for achieving higher efficiency, we often choose a security parameter that the previous asymptotic argument does not always make sense. For example, even if a cryptographic primitive yields 80-bit security in average over all possible choice of keys, there is still possibility that there exist weak keys such that an adversary can succeed in an attack with probability $2^{-60.5}$ for these keys and the probability of picking one of these keys is $2^{-20.5}$. For preventing picking such a weak key, one may use cryptographic primitives whose worst case security is proven to be equivalent to the average case security, or example, [3,4]. However, these schemes are generally less efficient than other practical schemes. Therefore, it is beneficial if we can somehow evaluate security under each specific key.

Unfortunately, when fixing a public key, it becomes absolutely infeasible to prove that there exists no effective adversary, which breaks the cryptographic primitive in any sense under the fixed key because it always exists in theory. Therefore, the best what we can do is just to use a public key such that its effective adversary is not likely to be constructed in the real life. Regarding this concept, Rogaway [5] proposed and formalized the notion of *human ignorance*, and investigate security of cryptographic primitives, for example, hash-then-sign signature, under the usage of collision-resistant hash function *without* the key, assuming that any effective adversary against the collision-resistant hash function (which always exists in theory) will never appear in the real life. The notion of human ignorance seems also useful for analyzing digital signature and/or public key encryption with the fixed key, and thus, it is desired to provide a method for evaluating the level of human ignorance of these cryptographic primitives.

1.2. Our results

1.2.0.1. Social Oracle and Fixed Key Security. Because for a fixed key, human and accidental factors significantly depend on the possibility of constructing an effective adversary (which potentially exists in theory) in the real life; it is hard to mathematically evaluate how likely it is. (For example, we can immediately find the discrete logarithm x if the given the instance is $g^x = g$ because we memorize $x = 1$ in such a case. This is not mathematical weakness but a human factor.) Thus, for investigating such possibility, we will model the human society as a massive Turing machine, which on input a program code of a cryptographic primitive and a fixed key, returns a program code of the most effective adversary against them among ones which human society can produce in the real life. We call this Turing machine *social oracle* $\mathcal{SO}$.

We define that a cryptographic primitive Π is *fixed key secure* (or human ignored [5]) in the sense of a security notion goal.atk on a fixed public key pk if for query $(\Pi, pk, \mathsf{goal.atk})$, the social oracle does not return any effective adversary with respect to goal.atk. From the property of the social oracle, we see that this is a reasonable definition of security under a fixed key. Now, our intention is to somehow predict the social oracle's answer $\mathcal{SO}(\Pi, pk, \mathsf{goal.atk})$ before querying $(\Pi, pk, \mathsf{goal.atk})$.

1.2.0.2. Impossiblitiy of Reducing to Weaker Notions. As our main result, roughly speaking, we show that there is no better method for forecasting $\mathcal{SO}(\Pi, pk, \mathsf{goal.atk})$ than the previous naive methods as long as we consider only black-box reductions if goal.atk represents a practical level of security. This also implies that the standard security notions, that is, EuF-CMA and IND-CCA, which take keys as random variables, are considered the most appropriate notions among what we can treat in practice.

More specifically, we investigate (in)feasibility of *narrowing* the space of adversarial strategies, which we have to take into account and show that it is absolutely impossible unless the program code of the adversary is explicitly used in analysis. Here, we say that the space of strategies can be *narrowed* if for knowing $\mathcal{SO}(\Pi, pk, \mathsf{goal.atk})$, it is sufficient to know $\mathcal{SO}(\Pi, pk, w\mathsf{goal.atk})$, where $w$goal.atk is a strictly weaker security notion than goal.atk in the sense that (Π, pk) is always vulnerable under the notion of goal.atk if it is vulnerable under the notion of $w$goal.atk, but not vice versa. For example, when the user wants to examine existential unforgeability (against any attack model) on his fixed key, if it is proven that he does not need to try forgery of a signature for a specific message, the space of adversarial strategies is considered narrowed.

Thus, our result can be interpreted that *for any digital signature scheme (resp. public key encryption scheme) and any fixed key, the de facto security notion, that is, existential unforgery against adaptive chosen message attacks (resp. indistinguishability against adaptive chosen ciphertext attacks), cannot be reduced to any weaker security notion if only black-box reductions are considered.* In other words, under black-box analysis, human ignorance of successful adversaries in the sense of the de facto security notion on a fixed key will never be implied by that of any weaker security notion on the same fixed key.

As a folklore, it is already (but informally) known that for any digital signature scheme (resp. public key encryption scheme) and any fixed key, security against

adaptive chosen message attacks (resp. adaptive chosen ciphertext attacks) cannot be reduced to security against key only attacks [6]. However, we stress that our impossibility results are significantly stronger than this because ours imply that there is completely *no* way for reducing the de facto security notion under a fixed key to *any* weaker notion under the same fixed key if we depend on only black-box analysis. Furthermore, our results take into account not only weaker notions but also a considerably wider range of security notions. Namely, loosely speaking, we show that it is also impossible to reduce the de facto security notion to any other notion, which is weaker in terms of *either* the adversarial goal *or* the attack model and, thus, as far as this condition is satisfied, even any stronger adversarial goal and attack model are addressed in our results. Furthermore, our results also imply that it is impossible to construct an adversary against any weaker security notion by using that against the de facto security notion in black-box manner *even if the latter's running time is considerably short*.

1.3. Related works

So far, possibility/impossibility results on cryptographic primitives have been intensively studies in the literatures. For example, in [7–11], it is shown that if one-way functions exist, then there also exist private key encryption, authentication, digital signature, bit commitment, and zero-knowledge proof. On the other hand, Impagliazzo and Rudich [12] considered various black-box settings and showed a black-box construction of key agreement based on one-way functions implies a proof that $P \neq NP$ in one model. Furthermore, in a more constrained model, they showed that the black-box construction is unconditionally impossible. A line subsequent works of [12] used their methodology or new variants to show black-box separations as follows. Kahn, Saks, and Smyth showed that a black-box separation between one-way functions and one-way permutations. Simon [13] showed that a black-box separation between one-way functions and collision-resistant hash functions. Gertner, Kannan, *et a*l. [14] and Gertner, Malkin, and Reingold [15] showed that a black-box separation among key agreement, oblivious transfer, public-key encryption, and trapdoor functions. Reingold, Trevisan, and Vadhan [16] reconsidered the results of [12], and strengthened some previous results. In [17–19], it is shown that black-box constructions suffer from inherent efficiency limitations.

All previous impossibility results cannot treat fixed key security. The previous results related to our paper (but does not focus on fixed key security) are as follows. In [5], Rogaway introduced a novel direction of studying impossibility/possibility for treating cryptographic primitives that always theoretically exist but are not likely to be constructed in the real world and called this notion *human ignorance*. Furthermore, for discussing such kind of primitives, he addressed that it is important to (not merely give a security proof but) explicitly construct an adversary, which breaks the basic primitive whose effective adversaries are considered human ignored. For investigating (im)possibility of (extensions of) black-box reductions, Paillier *et al*. presented some useful techniques in [20–22]. For example, in [20], (im)possibility results for discrete log-based signatures (e.g., Schnorr signature) under discrete log, and one more discrete log assumptions are shown. Because we address a class of human ignorance, similar techniques (i.e., meta-reduction techniques under key-preserving black-box reductions) to theirs are also used in this paper. More recently, impossibility results based on meta-reductions techniques have appeared in a number of works, for exmaple, [23–33], to name a few. See [34] for a good survey on this topic. Fischlin and Fleischhacker [29] showed a limitation on the meta-reduction techniques.

2. PRELIMINARIES

2.1. Real-life adversaries

In this paper, for simplicity, we assume that all keys are generated at time 0 and their life time is ended at time T. Then, we say that an Algorithm A is a *real-life adversary* if it is explicitly implemented at some time T' such that $0 \leq T' < T$ and its running time is less than $T - T'$. We also say that an Algorithm A is a α*-practical adversary* if it is explicitly implemented at some time T' such that $0 \leq T' < \alpha T$ and its running time is less than $\alpha T - T'$, where $0 < \alpha \leq 1$. Obviously, a one-practical adversary is a real-life adversary, and an α-practical adversary is always a β-practical adversary for all α and β such that $\alpha \leq \beta$. Roughly speaking, α-practical adversaries are a powerful class of real-life adversaries that succeed in the attack significantly earlier than T. Consequently, even if it is proven to be generally impossible to construct a real-life adversary against some weaker security notion from that against the de facto security notion, it might be still possible to construct the former from an α-practical adversary against the de facto security notion.

2.2. Digital signature and public key encryption

A digital signature scheme is given by a triple of algorithms, $\Sigma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$. Gen, the key generation algorithm, takes as input a security parameter, and returns a pair (pk, sk) of matching public and secret keys. Sig, the signature generation algorithm, takes as inputs a secret key sk and a message m and returns a signature $\sigma = \mathsf{Sig}_{sk}(m)$. Ver, the verification algorithm, takes as inputs a public key, a message, and a signature and outputs 1 if and only if σ is valid on m, or 0 otherwise.

A public key encryption scheme is given by a triple of algorithms, $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$. Gen, the key generation algorithm, takes as inputs a security parameter, and returns a pair (pk, sk) of matching public and secret keys.

Enc, the encryption algorithm, takes as inputs a public key pk and a plaintext m and returns a ciphertext $c = \mathsf{Enc}_{pk}(m)$. Dec, the decryption algorithm, is a deterministic algorithm, which takes as inputs a secret key sk and a ciphertext c and outputs a plaintext $m = \mathsf{Dec}_{sk}(c)$ or a special symbol $\perp$, which indicates that the ciphertext was invalid.

2.3. Security notions for digital signature and public key encryption

Security notions for a digital signature scheme are defined by pairing an adversarial goal (goal) and an attack model (atk) [6]. We first review the three main adversarial goals (goal) for (Σ, pk) where Σ is a digital signature scheme and pk is a public key of Σ. (1)**Total unBreakable** (tub): (Σ, pk) is said to be tub when no real-life adversary can compute the secret key sk, which corresponds to pk. (2)**Universal unforgery** (uuf): (Σ, pk) is said to be uuf when for a randomly chosen message m^* from the message space $\mathcal{M}$, no real-life adversary can forge a valid signature σ^* on m^*. (3)**Existential unforgery** (euf): (Σ, pk) is said to be euf when no real-life adversary can forge a pair of a message m^* and its valid signature σ^*.

Three main attack models (atk) for (Σ, pk) are as follows. (i)**Key only attack**: In this model, an adversary is allowed to access the empty oracle ε, which for any input, return $\perp$. (ii)**Known message attack** (kma): In this model, an adversary is allowed to access the restrictive signing oracle $\mathcal{RS}$, which on input 0, returns a pair of a message m and its signature $\sigma = \mathsf{Sig}_{sk}(m)$ where m is chosen from a pre-determined distribution.† (iii) **Chosen message attack** (cma): In this model, an adversary is allowed to access the signing oracle $\mathcal{S}$, which on input a message m returns its signature $\sigma = \mathsf{Sig}_{sk}(m)$. The previous goals are considered not achieved if the adversary submits a query whose answer from the oracle can be trivially transformed into the correct output.

We remark that the adversarial goals and attack models, which are mentioned in this section, are only particular examples, and (in)feasibility results in this paper take into account all possible adversarial goals and attack models for both digital signature and public key encryption.

Similarly to the case of digital signatures, security notions for public key encryption schemes are defined by pairing an adversarial goal (goal) and an attack model (atk) [35–37]. We review three main adversarial goals (goal) for (Π, pk) where Π is a public key encryption scheme and pk is a public key of Π. (i) **Total unBreakable** (tub): (Π, pk) is said to be tub when no real-life adversary can compute the secret key sk, which corresponds to pk. (2)**One-wayness** (ow): (Π, pk) is said to be ow when for a given ciphertext $c^* = \mathsf{Enc}_{pk}\left(m^*\right)$ where m^* is a randomly chosen plaintext from the plaintext space $\mathcal{M}$, no real-life adversary can recover m^*. (3)**Indistinguishability** (ind): (Π, pk) is said to be ind when for a given ciphertext $c_b = \mathsf{Enc}_{pk}(m_b)$ where a plaintext $m_b \in \{m_0, m_1\}$ and (m_0, m_1) are chosen by the adversary, no real-life adversary can output $b' = b$ with a meaningfully higher probability than one-half.

Three main attack models (atk) for (Π, pk) are as follows. (1)**Chosen plaintext attack** (cpa): In this model, an adversary is allowed to access the empty oracle ε, which for any input, returns $\perp$. (ii) **Plaintext checking attack** (pca, [37]): In this model, an adversary is allowed to access the plaintext-checking oracle $\mathcal{C}$, which on input (m, c), returns 1 if $m = \mathsf{Dec}_{sk}(c)$, otherwise returns 0. (3)**Chosen ciphertext attack** (cca): In this model, an adversary is allowed to access the decryption oracle $\mathcal{D}$, which on input a ciphertext c, returns a plaintext $m = \mathsf{Dec}_{sk}(c)$ or a special symbol $\perp$, which indicates that the ciphertext was invalid. The previous goals are considered not achieved if the adversary submits a query whose answer from the oracle can be trivially transformed into the correct output.

3. FIXED KEY SECURITY

3.1. Social oracle and fixed key security

As we mentioned, in the real usage of digital signature or public key encryption schemes, a user is more interested in the security under a specific key, which he is using as his public key, rather than the average security under randomly chosen keys. We call a real-life adversary, which successfully breaks cryptographic primitive X in the sense of goal.atk under (only) a specific public key pk a *fixed key* goal.atk *adversary on* (X, pk). Here, we say that an adversary *breaks* X in the sense of goal.atk if it succeeds in achieving adversarial goal goal in attack model atk with probability more than $C \cdot P_{min} + P_c$ where P_{min} is the minimum non-negligible value *in practice*‡ (with respect to the life time of pk), C is some constant, and P_c is probability of succeeding in the attack by random guess. Throughout this paper, we assume that $1 \gg P_{min} \gg 1/2^k$ where k is the security parameter, and that an event which occurs with probability less than P_{min} will never occur in practice. It is obvious that for all pk, there always exists such a fixed key adversary, potentially. However, this does not immediately imply that for a fixed pk, a successful fixed key adversary can be always *constructed* in the real world.

For investigating possibility that such a fixed key adversary actually appears in the real world, we first define fixed key adversaries as follows.

† Rigorously, it is necessary to specify the distribution of the messages for defining kma, but since our results hold for any distribution, here we do not strictly specify it.

‡ This value also depends on human factors. For example, if computation of at most λ-bit complexity will become feasible at the end of the life time of pk, then we can set $P_{min} = 1/2^{\lambda}$.

Definition 1. *Let* $\Sigma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ *be a digital signature scheme and pk be a public key of* Σ. *We say that an Algorithm A is a fixed-key* goal.atk *adversary (resp. an* α*-strong fixed-key* goal.atk *adversary) on* (Σ, pk) *if it is a real-life adversary (resp.* α*-practical adversary), and the following probability is equal to or larger than* $C{\cdot}P_{min}{+}P_c$*:* $\Pr[x \leftarrow A^{\mathcal{O}_{\mathsf{atk}}}(y)]$ *where* (C, P_c, x, y) *and* $\mathcal{O}_{\mathsf{atk}}$ *are determined by* goal *and* atk*, respectively. For example,* $(C, P_c, x, y) = (1, 0, sk, pk)$, $\left(1, 0, \sigma^*, (pk, m^*)\right)$ *such that* $m^* \overset{\$}{\leftarrow} \mathcal{M}$, *or* $\left(1, 0, (m^*, \sigma^*), pk\right)$ *if* goal=tub, uuf, *or* euf*, respectively, and* $\mathcal{O}_{\mathsf{atk}} = \varepsilon, \mathcal{RS}$, *or* $\mathcal{S}$ *if* atk=*koa,* kma, *or* cma*, respectively (see Section 2.2 for notations).*

Similarly, fixed key adversaries for public key encryption schemes are defined as follows.

Definition 2. *Let* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *be a public key encryption scheme and pk be a public key of* Π. *We say that an Algorithm A is a fixed-key* goal.atk *adversary (resp. an* α*-strong fixed-key* goal.atk *adversary) on* (Π, pk) *if it is a real-life adversary (resp. an* α*-practical adversary) and the following probability is equal to or larger than* $C{\cdot}P_{min}{+}P_c$*:* $\Pr[(m_0, m_1, state) \leftarrow A^{\mathcal{O}_{\mathsf{atk}}}(pk); b \overset{\$}{\leftarrow} \{0,1\}; c_b = \mathsf{Enc}_{pk}(m_b) : x \leftarrow A^{\mathcal{O}_{\mathsf{atk}}}(y)]$ *where* (C, P_c, x, y) *and* $\mathcal{O}_{\mathsf{atk}}$ *are determined by* goal *and* atk*, respectively. For example,* $(C, P_c, x, y) = (1, 0, sk, pk)$, $\left(1, 0, m^*, (pk, c^*)\right)$ *such that* $m^* \overset{\$}{\leftarrow} \mathcal{M}$ *and* $c^* = \mathsf{Enc}_{pk}\left(m^*\right)$, *or* $(1/2, 1/2, b, (pk, c_b, state))$ *if* goal = tub, ow, *or* ind *respectively, and* $\mathcal{O}_{\mathsf{atk}} = \varepsilon, \mathcal{C}$, *or* $\mathcal{D}$ *if* atk=cpa, pca, *or* cca*, respectively (See Section 2.3. for notations).*

In what follows, $\mathcal{A}_{\mathsf{goal.atk}[X,pk]}$ and $\mathcal{A}_{\alpha\text{–}\mathsf{goal.atk}[X,pk]}$ denote the set of all fixed-key goal.atk adversaries on (X, pk) and that of all α-strong fixed-key goal.atk adversaries on (X, pk), respectively, where X is a digital signature scheme or a public key encryption scheme and pk is a public key of X.

Next, we define the presence/absence of fixed-key adversaries in the real world by introducing *social oracle* $\mathcal{SO}$, which models the human society as a massive Turing machine. For a query $(X, pk, \mathsf{goal.atk})$ where X is a digital signature scheme or a public key encryption scheme, pk is a public key of X, and goal.atk is a security notion; $\mathcal{SO}$ returns a successful fixed-key goal.atk adversary on (X, pk) if and only if it will be actually constructed in the real world. The social oracle is formally defined as follows.

Definition 3 (Social Oracle)**.** *Define that social oracle* $\mathcal{SO}$ *works as follows.*

- *For a query* $(X, pk, \mathsf{goal.atk})$ *where X, pk, and* goal.atk *are a digital signature scheme or a public key encryption scheme, a public key of X, and a security notion, respectively;* $\mathcal{SO}$ *returns a program code of an Algorithm* $A \in \mathcal{A}_{\mathsf{goal.atk}[X,pk]}$, *which breaks X in the sense that* goal.atk *will be actually implemented at time* T' *for some* $T'(< T)$ *and its running time is less than* $T - T'$ *(Section 2.1). It returns* $\perp$ *otherwise.*
- *Assume that for a given real-life adversary* $A_1 \in \mathcal{A}_{\mathsf{goal1.atk1}[X,pk]}$, *it is always possible to construct another real-life adversary* A_2 *such that* $A_2 \in \mathcal{A}_{\mathsf{goal2.atk2}[X,pk]}$. *Then, if* $\mathcal{SO}(X, pk, \mathsf{goal1.atk1})$ *outputs a program code of an Algorithm* $\overline{A}_1$ *such that* $\overline{A}_1 \in \mathcal{A}_{\mathsf{goal1.atk1}[X,pk]}$, $\mathcal{SO}(X, pk, \mathsf{goal2.atk2})$ *always outputs that of another Algorithm* $\overline{A}_2$ *such that* $\overline{A}_2 \in \mathcal{A}_{\mathsf{goal2.atk2}}[X, pk]$.

The second property of $\mathcal{SO}$ seems always provided if the first property is satisfied, and thus, the second property might be redundant. However, we require this condition for proving our main theorems and, therefore, explicitly address it in the definition. Now, fixed security can naturally be defined as follows.

Definition 4 (Fixed Key Security)**.** *Let X and pk be a digital signature scheme or a public key encryption scheme, and a public key of X, respectively. We say that* (X, pk) *is* goal.atk *secure if* $\mathcal{SO}(X, pk, \mathsf{goal.atk})$ *only outputs* $\perp$.

3.2. Naive methods for analyzing fixed key security

In the mentioned text earlier, we define that (X, pk) is fixed key secure (i.e., human ignored) if the social oracle does not output any program code, which harms security of (X, pk). A naive method for forecasting the answer from the social oracle is to verify existence of vulnerability for *each* of *all* feasible adversarial strategies. Because, of course, it is considered impossible in practice, actually the best what we can do is only to verify that for *each* of a *subset* of *all* feasible adversarial strategies. Generally, this subset is a tiny part of all feasible strategies, and consequently, even if no vulnerability is found out by the previous method, this is only a very weak evidence that (X, pk) is fixed key secure. For example, if we want to know whether (Σ, pk) is euf.cma secure or not, we have to verify possibility of signature forgery for each of *all* messages, which can be potentially signed under each of *all* combinations of signing queries. Obviously, it is impossible to encompass all of the feasible strategies, and only a tiny part of them can be verified.

For strengthening the previous naive method, next, we consider possibility of narrowing the space of all feasible strategies. Namely, if the number of all feasible strategies is decreased, it becomes possible to encompass a larger part of them. Because the decrease of the number of all strategies means that the security notion is weakened, the mentioned text earlier can be interpreted that *if* goal1.atk1, *security on* (X, pk) *can be reduced to another weaker security notion* goal2.atk2 *on* (X, pk) *and any vulnerability in the sense of* goal2.atk2 *is not discovered as*

far as we can examine; this fact can be a stronger evidence of goal1.atk1 *security on* (X, pk) *than that by the previous naive method.* For example, if euf.cma security on (Σ, pk) can be reduced to uuf.cma security on (Σ, pk), then we have to verify possibility of only signature forgery for a specific message under each of *all* combinations of signing queries, and it is considered that the space of all feasible strategies is significantly narrowed.

Our main result is that unfortunately, it is impossible to reduce euf.cma security on *any* (Σ, pk) to any weaker fixed key security on (Σ, pk) under black-box analysis. Similarly, it is also impossible to reduce ind.cca security on *any* (Π, pk) to any weaker fixed key security on (Π, pk) under black-box analysis. *These results imply that for evaluating* euf.cma *security or* ind.cca *security, there is no better method than the previous naive method as long as we consider only black-box reductions.*

For formally stating these results, we address the definition of fixed key black-box reduction as follows.

Definition 5 (Fixed Key Black-box Reduction)**.** *We say that an oracle Turing machine R is a fixed key black-box (FKBB) reduction from a fixed key* goal1.atk1 *adversary on* (X, pk) *to a fixed key* goal2.atk2 *adversary on* (X, pk) *if for every* $A_2 \in \mathcal{A}_{\mathsf{goal2.atk2}[X,pk]}$, $R^{A_2} \in \mathcal{A}_{\mathsf{goal1.atk1}[X,pk]}$ *always holds. We denote this by* $\mathcal{A}_{\mathsf{goal1.atk1}[X,pk]} \Leftarrow_R \mathcal{A}_{\mathsf{goal2.atk2}[X,pk]}$. *We also say that an oracle Turing machine R is a* α*-weak FKBB reduction from a fixed key* goal1.atk1 *adversary on* (X, pk) *to an* α*-strong fixed key* goal2.atk2 *adversary on* (X, pk) *if for every* $A_2 \in \mathcal{A}_{\alpha\text{–}\mathsf{goal2.atk2}[X,pk]}$, $R^{A_2} \in \mathcal{A}_{\mathsf{goal1.atk1}[X,pk]}$ *always holds. We denote this by* $\mathcal{A}_{\mathsf{goal1.atk1}[X,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{goal2.atk2}[X,pk]}$.

We notice that an FKBB reduction has the transitive property. For instance, for given implementations of an α-weak FKBB reduction R_1 and an FKBB reduction R_2 such that $\mathcal{A}_{\mathsf{goal1.atk1}[X,pk]} \Leftarrow_{R_1} \mathcal{A}_{\alpha\text{–}\mathsf{goal2.atk2}[X,pk]}$ and $\mathcal{A}_{\mathsf{goal3.atk3}[X,pk]} \Leftarrow_{R_2} \mathcal{A}_{\mathsf{goal1.atk1}[X,pk]}$, it is always possible to explicitly construct another α-weak FKBB reduction R_3 such that $\mathcal{A}_{\mathsf{goal3.atk3}[X,pk]} \Leftarrow_{R_3} \mathcal{A}_{\alpha\text{–}\mathsf{goal2.atk2}[X,pk]}$. For such R_1, R_2, and R_3, we denote $R_3 = R_1 \circ R_2$.

Based on Definition 5, we can naturally define (in)comparability of security notions as follows.

Definition 6 ((In)Compatibility of Security Notions)**.** *We say that* goal1 *is harder (resp. easier) than* goal2 *if for all* (X, pk) *and* atk*, it is always possible to explicitly construct an FKBB reduction R such that* $\mathcal{A}_{\mathsf{goal2.atk}[X,pk]} \Leftarrow_R \mathcal{A}_{\mathsf{goal1.atk}[X,pk]}$ *(resp.* $\mathcal{A}_{\mathsf{goal1.atk}[X,pk]} \Leftarrow_R \mathcal{A}_{\mathsf{goal2.atk}[X,pk]}$*) and that* goal1 *is incomparable with respect to* goal2 *if* goal1 *is not harder nor easier than* goal2*. Similarly, we say that* atk1 *is weaker (resp. stronger) than* atk2 *if for all* (X, pk) *and* goal*, it is always possible to explicitly construct an FKBB reduction R such that* $\mathcal{A}_{\mathsf{goal.atk2}[X,pk]} \Leftarrow_R \mathcal{A}_{\mathsf{goal.atk1}[X,pk]}$ *(resp.* $\mathcal{A}_{\mathsf{goal.atk1}[X,pk]} \Leftarrow_R \mathcal{A}_{\mathsf{goal.atk2}[X,pk]}$*) and that* atk1 *is incomparable with respect to* atk2 *if* atk1 *is not weaker nor stronger than* atk2*.*

In Section 4, we show that for all (Σ, pk) and for all goal.atk, it is impossible to construct any FKBB reduction from a fixed key goal.atk adversary to a fixed key euf.cma adversary if goal is harder than euf and atk is weaker than cma. Similarly, in Section 5, we show that for all (Π, pk), for all goal.atk, it is impossible to construct any FKBB reduction from a fixed key goal.atk adversary to a fixed key ind.cca adversary if goal is harder than ind and atk is weaker than cca. In these sections, we further clarify that our impossibility results can be applicable to a significantly wider range of security notions.

4. IMPOSSIBILITY OF FIXED KEY BLACK-BOX REDUCTION FOR DIGITAL SIGNATURE

In this section, loosely speaking, we show that it is impossible to construct any FKBB reduction R such that $\mathcal{A}_{\mathsf{goal.atk}[\Sigma,pk]} \Leftarrow_R \mathcal{A}_{\mathsf{euf.cma}[\Sigma,pk]}$ for all digital signature scheme Σ, all public key pk, and all goal.atk if goal is harder than euf *or* atk is weaker than cma. More specifically, the following three facts are clarified: (i) for all (Σ, pk) and goal.atk, it is impossible to construct any R such that $\mathcal{A}_{\mathsf{goal.atk}[\Sigma,pk]} \Leftarrow_R \mathcal{A}_{\mathsf{euf.cma}[\Sigma,pk]}$ if goal is harder than euf, atk is weaker than cma, and (Σ, pk) is goal.atk secure (Theorem 1), (ii) for all (Σ, pk) and goal.atk, it is impossible to construct any R such that $\mathcal{A}_{\mathsf{goal.atk}[\Sigma,pk]} \Leftarrow_R \mathcal{A}_{\mathsf{euf.cma}[\Sigma,pk]}$ if goal is easier than uuf, atk is weaker than cma, and (Σ, pk) is goal.atk secure (Theorem 2), and (iii) for all (Σ, pk) and goal.atk, it is impossible to construct any R such that $\mathcal{A}_{\mathsf{goal.atk}[\Sigma,pk]} \Leftarrow_R \mathcal{A}_{\mathsf{euf.cma}[\Sigma,pk]}$ if goal is harder than euf, atk is stronger than kma, and (Σ, pk) is goal.atk secure (Theorem 3). In Appendix A, we summarize the previous results in Table A1.

The previous three results intuitively imply that for all (Σ, pk) and goal.atk, it is impossible to construct any R such that $\mathcal{A}_{\mathsf{goal.atk}[\Sigma,pk]} \Leftarrow_R \mathcal{A}_{\mathsf{euf.cma}[\Sigma,pk]}$ if goal is harder than euf *or* atk is weaker than cma. Actually, this is almost true (assuming that (Σ, pk) is fixed key goal.atk secure), and exceptions are only the following cases: (i) atk is weaker than cma, but goal is incomparable with respect to uuf, and (ii) goal is harder than euf, but atk is incomparable with respect to kma. For example, partial recovery of the secret key (as an adversarial goal) may be incomparable with respect to uuf. In Table A1, we summarize the previous results.

Theorem 1. *For all* (Σ, pk) *where* Σ *is a digital signature scheme and pk is a public key of* Σ*, and for all* goal.atk *where* goal.atk *is a security notion such that* goal *is harder than* euf*, and* atk *is weaker than* cma*, if* (Σ, pk) *is* goal.atk *secure, for all* α $(0 < \alpha \leq 1)$*, it is*

DOI: 10.1002/sec

impossible to construct even any α-weak FKBB reduction R such that $\mathcal{A}_{\mathsf{goal.atk}[\Sigma,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{euf.cma}[\Sigma,pk]}$.

Proof. For proving the theorem, we first address the following lemma. □

Lemma 1. *For all* (Σ, pk) *and* atk *such that* atk *is weaker than* cma*, if* (Σ, pk) *is* euf.atk *secure, for all* α $(0 < \alpha \leq 1)$ *it is impossible to construct any α-weak FKBB* R' *such that* $\mathcal{A}_{\mathsf{euf.atk}[\Sigma,pk]} \Leftarrow_{R'} \mathcal{A}_{\alpha\text{–}\mathsf{euf.cma}[\Sigma,pk]}$.

Lemma 1 (and its proof) implies that if it is possible to prove $\mathsf{euf.cma}[\Sigma, pk]$ security under the assumption that $\mathsf{euf.atk}[\Sigma, pk]$ is guaranteed, we can always explicitly construct a practical adversary, which can break $(\Sigma, pk]$) in the sense of $\mathsf{euf.atk}[\Sigma, pk]$. Obviously, this is a contradiction and thus, we can conclude that FKBB reduction R' such that $\mathcal{A}_{\mathsf{euf.atk}[\Sigma,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{euf.cma}[\Sigma,pk]}$ does not exist if (Σ, pk) is euf.atk secure.

Proof of Lemma 1. Towards a contradiction, we assume that for some α, an implementation of an α-weak FKBB R such that $\mathcal{A}_{\mathsf{euf.atk}[\Sigma,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{euf.cma}[\Sigma,pk]}$ is given. Then, the theorem is proven by constructing a fixed key euf.atk adversary B on (Σ, pk).

We can construct such B by using R as follows. B first activates R, and then, R starts interacting with a (virtual) oracle $\mathcal{O}_{\mathsf{atk}}$ (which is determined by atk) and a (virtual) fixed key euf.cma adversary on (Σ, pk). When R submits a query to the virtual $\mathcal{O}_{\mathsf{atk}}$, B responds to it in such a way that B submits the same query to his own $\mathcal{O}_{\mathsf{atk}}$ and returns the answer from $\mathcal{O}_{\mathsf{atk}}$ as it is. On the other hand, B does not need to simulate the euf.cma adversary until R correctly answers to all queries from B who pretends as the euf.cma adversary. Therefore, R's view is perfectly indistinguishable from the normal communication with $\mathcal{O}_{\mathsf{atk}}$ and an euf.cma adversary.

Because for all $A \in \mathcal{A}_{\alpha\text{–}\mathsf{euf.cma}[\Sigma,pk]}$, R^A breaks (Σ, pk) in the sense of euf.atk, but R itself cannot (if it can, this contradicts that (Σ, pk) is euf.atk secure); it is guaranteed that R correctly answers to all queries from B with probability more than P_{min}. This is because there may exist a real fixed key euf.cma adversary, which will output nothing unless all of his queries are correctly answered, and therefore, R has to succeed in simulating the real attack environment with probability more than P_{min} (because if it fails, R has to break (Σ, pk) by itself alone). Hence, B obtains at least one valid signed message (m^*, σ^*) by interacting with R with probability more than P_{min}, and furthermore, (m^*, σ^*) is always available as B's output (by carefully choosing queries to R).

Finally, we confirm whether B is a real-life adversary or not. Because B can be immediately implemented if any implementation of $A \in \mathcal{A}_{\alpha\text{–}\mathsf{euf.cma}[\Sigma,pk]}$ is given, thus assuming that A is implemented at time $T'(< \alpha T)$ and B is implementable at time T' as well. Furthermore, B's running time is the same as that of R because B does nothing except for invoking R, and R's running time is estimated at most $T - T'$. Notice that by definition, R^A's running time is at most $T - T'$, and consequently, R's running time is less than $T - T'$. Hence, B's running time is also at most $T - T'$, and it is a real-life adversary.

Therefore, B works as a successful fixed key euf.atk adversary, and it can be explicitly constructed if we are given any implementation of R such that $\mathcal{A}_{\mathsf{euf.atk}[\Sigma,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{euf.cma}[\Sigma,pk]}$. And this contradicts to the assumption that (Σ, pk) is euf.atk secure. □

Next, we address the following lemma, which can be trivially proven by definition.

Lemma 2. *For all* (Σ, pk) *and* goal.atk *such that* goal *is harder than* euf*, it is always possible to construct an FKBB reduction R such that* $\mathcal{A}_{\mathsf{euf.atk}[\Sigma,pk]} \Leftarrow_R \mathcal{A}_{\mathsf{goal.atk}[\Sigma,pk]}$.

Because of Lemma 2, it is guaranteed that an FKBB R' such that $\mathcal{A}_{\mathsf{euf.atk}[\Sigma,pk]} \Leftarrow_{R'} \mathcal{A}_{\mathsf{goal.atk}[\Sigma,pk]}$ can be explicitly constructed. Therefore, if an α-weak FKBB reduction R such that $\mathcal{A}_{\mathsf{goal.atk}[\Sigma,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{euf.cma}[\Sigma,pk]}$ can be constructed, then by transitivity, another α-weak FKBB reduction $R'' = R \circ R'$ such that $\mathcal{A}_{\mathsf{euf.atk}[\Sigma,pk]} \Leftarrow_{R''} \mathcal{A}_{\alpha\text{–}\mathsf{euf.cma}[\Sigma,pk]}$ can be always constructed as well. Furthermore, assuming that an implementation of such an R is given, (Σ, pk) is euf.cma secure if (Σ, pk) is goal.atk secure, and this implies that (Σ, pk) is euf.atk secure if (Σ, pk) is goal.atk secure because atk is weaker than cma. However, because of Lemma 1, it is shown to be impossible to construct such R'' if (Σ, pk) is euf.atk secure, and thus, R cannot be constructed neither, which proves the theorem.

The previous theorem does not merely mention impossibility for constructing a fixed key goal.atk adversary from a fixed euf.cma adversary but a significantly stronger result implicating that it is impossible to construct the former even if a very efficient implementation of the latter is used. In other words, even if (Σ, pk) is likely to be safe in the sense of goal.atk, this does not imply that even powerful euf.cma adversaries with very short running time will not appear. Other theorems in this paper also state similar strong impossibility results.

Theorem 2. *For all* (Σ, pk) *where* Σ *is a digital signature scheme and pk is a public key of* Σ *and for all* goal.atk *where* goal.atk *is a security notion such that* goal *is easier than* uuf *(and thus, may be easier than or even incomparable with respect to* euf*) and* atk *is weaker than* cma*, if* (Σ, pk) *is* goal.atk *secure, for all* α $(0 < \alpha \leq 1)$*, it is impossible to construct even any α-weak FKBB reduction R such that* $\mathcal{A}_{\mathsf{goal.atk}[\Sigma,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{euf.cma}[\Sigma,pk]}$.

Proof. This theorem can be proven in a similar manner to Lemma 1. We assume that an implementation of α-weak FKBB R such that $\mathcal{A}_{\mathsf{goal.atk}[\Sigma,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{euf.cma}[\Sigma,pk]}$

is given. Then, the theorem is proven by constructing a real-life adversary B, which breaks (Σ, pk) in the sense of uuf.atk (not goal.atk). Namely, if B is an implementation of a fixed key uuf.atk adversary on (Σ, pk), then by using B, it is also possible to construct a fixed key goal.atk adversary on (Σ, pk) for all goal such that goal is easier than uuf.

B first activates R, and then, R starts interacting with a (virtual) oracle $\mathcal{O}_{\mathsf{atk}}$ (which is determined by atk) and a (virtual) α-strong fixed key euf.cma adversary on (Σ, pk). When R submits a query to the virtual $\mathcal{O}_{\mathsf{atk}}$, B responds to it in such a way that B submits the same query to his own $\mathcal{O}_{\mathsf{atk}}$ and returns the answer from $\mathcal{O}_{\mathsf{atk}}$ as it is. On the other hand, B does not need to simulate the α-strong fixed key euf.cma adversary until R correctly answers to all queries from B who pretends as the α-strong fixed key euf.cma adversary. Therefore, R's view is perfectly indistinguishable from the normal communication with $\mathcal{O}_{\mathsf{atk}}$ and an α-strong fixed key euf.cma adversary.

Similarly to the proof of Lemma 1, B works as a successful fixed key uuf.atk adversary, and it can be explicitly constructed if we are given any implementation of R such that $\mathcal{A}_{\mathsf{euf.atk}[\Sigma,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{euf.cma}[\Sigma,pk]}$, which contradicts to the assumption that (Σ, pk) is goal.atk secure (because goal is easier than uuf). □

Theorem 3. *For all* (Σ, pk) *where* Σ *is a digital signature scheme and pk is a public key of* Σ *and for all* goal.atk *where* goal.atk *is a security notion such that* goal *is harder than* euf *and* atk *is stronger than* kma *(and thus, may be stronger than or even incomparable with respect to* cma*), if* (Σ, pk) *is* goal.atk *secure, for all* α $(0 < \alpha \leq 1)$, *it is impossible to construct even any* α*-weak FKBB reduction R such that* $\mathcal{A}_{\mathsf{goal.atk}[\Sigma,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{euf.cma}[\Sigma,pk]}$.

Proof. This theorem can be proven in a slightly different manner from Lemma 1 and Theorem 2. We assume that an implementation of an α-weak FKBB R such that $\mathcal{A}_{\mathsf{goal.atk}[\Sigma,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{euf.cma}[\Sigma,pk]}$ is given. Then, the theorem is proven by constructing a real-life adversary B, which breaks (Σ, pk) in the sense of goal.atk. Let (C, P_c, x, y) be the constant value, the probability of succeeding in the attack by random guess, the correct output, and the input to the adversary, which are determined by atk (see Definition 1 for details).

B first activates R and inputs y to R. Then, R starts interacting with a (virtual) oracle $\mathcal{O}_{\mathsf{atk}}$ (which is determined by atk) and a (virtual) α-strong fixed key euf.cma adversary on (Σ, pk). When R submits a query to the virtual $\mathcal{O}_{\mathsf{atk}}$, B responds to it in such a way that B submits the same query to his own $\mathcal{O}_{\mathsf{atk}}$ and returns the answer from $\mathcal{O}_{\mathsf{atk}}$ as it is. On the other hand, B does not need to simulate the α-strong fixed key euf.cma adversary until R correctly answers to all queries from B who pretends as the α-strong fixed key euf.cma adversary. Therefore, R's view is perfectly indistinguishable from the normal communication with $\mathcal{O}_{\mathsf{atk}}$ and an α-strong fixed key euf.cma adversary.

At some point, B (who is simulating an α-strong fixed key euf.cma adversary) is enforced to return a valid signed message to R. Then, B invokes an FKBB reduction $\overline{R}$ such that $\mathcal{A}_{\mathsf{goal.atk}[\Sigma,pk]} \Leftarrow_{\overline{R}} \mathcal{A}_{\mathsf{goal.kma}[\Sigma,pk]}$. Because atk is stronger than kma, such an $\overline{R}$ can be always constructed. B next activates $\overline{R}$, and then, $\overline{R}$ starts interacting with a (virtual) oracle $\mathcal{O}_{\mathsf{atk}}$ and a (virtual) fixed key goal.kma adversary on (Σ, pk). When $\overline{R}$ submits a query to the virtual $\mathcal{O}_{\mathsf{atk}}$, B responds to it by interacting with his own $\mathcal{O}_{\mathsf{atk}}$. On the other hand, B does not need to simulate the goal.kma adversary until $\overline{R}$ correctly answers to all queries. We note that $\overline{R}$'s view is perfectly indistinguishable from the normal communication with $\mathcal{O}_{\mathsf{atk}}$ and an goal.kma adversary.

Because for all $A \in \mathcal{A}_{\mathsf{goal.kma}[\Sigma,pk]}$, $\overline{R}^A$ breaks (Σ, pk) in the sense of goal.atk, but $\overline{R}$ itself cannot (if it can, this contradicts to the assumption that (Σ, pk) is goal.atk secure); it is guaranteed that $\overline{R}$ correctly answers to all queries from B (i.e., simulates the restrictive signing oracle $\mathcal{RS}$) with probability more than P_{min}. Hence, B obtains at least one valid signed message (m^*, σ^*) by interacting with $\overline{R}$ with probability more than P_{min}, and furthermore, (m^*, σ^*) is always available as B's output. We note that this is existential forgery because m^* is randomly chosen from the pre-determined distribution. Finally, B returns (m^*, σ^*) to R as the output of the simulated α-strong fixed key euf.cma adversary.

From R's view, B perfectly simulates a successful α-strong fixed key euf.cma adversary (because its success probability is more than P_{min}), and consequently, R eventually outputs the correct x with probability more than $C \cdot P_{min} + P_c$. B finally outputs the same value.

Similarly to the proof of Lemma 1, we see that B works as a fixed key goal.atk adversary, which contradicts to the assumption that (Σ, pk) is goal.atk secure. □

5. IMPOSSIBILITY OF FIXED KEY BLACK-BOX REDUCTION FOR PUBLIC KEY ENCRYPTION

In this section, we discuss the impossibility of FKBB reduction for the case of public key encryption. In contrast to the case of euf for digital signature, P_c in ind for public key encryption is one-half, and this results in the significant difference in the proofs of the impossibility results. Nevertheless, the obtained results are similar. Namely, roughly speaking, we show that it is impossible to construct any FKBB reduction R such that $\mathcal{A}_{\mathsf{goal.atk}[\Pi,pk]} \Leftarrow_R \mathcal{A}_{\mathsf{ind.cca}[\Pi,pk]}$ for all public key encryption scheme Π, all public key pk, and all goal.atk if goal is harder than ind *or* atk is weaker than cca.

In Appendix A, we summarize the previous results in Table A2. Proofs of theorems are given in Appendix B.

Theorem 4. *For all* (Π, pk) *where* Π *is a public key encryption scheme and pk is a public key of* Π *and for*

all goal.atk *where* goal.atk *is a security notion such that* goal *is harder than* ind *and* atk *is weaker than* cca*, if* (Π, pk) *is* goal.atk *secure, for all* α $(0 < \alpha \leq 1)$*, it is impossible to construct even any* α*-weak FKBB reduction* R *such that* $\mathcal{A}_{\mathsf{goal.atk}[\Pi,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{ind.cca}[\Pi,pk]}$.

Theorem 5. *For all* (Π, pk) *where* Π *is a public key encryption scheme and* pk *is a public key of* Π *and for all* goal.atk *where* goal.atk *is a security notion such that* goal *is easier than* ow *(and thus, may be easier than or even incomparable with respect to* ind*) and* atk *is weaker than* cca*, if* (Π, pk) *is* goal.atk *secure, for all* α $(0 < \alpha \leq 1)$*, it is impossible to construct even any* α*-weak FKBB reduction* R *such that* $\mathcal{A}_{\mathsf{goal.atk}[\Pi,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{ind.cca}[\Pi,pk]}$.

Theorem 6. *For any* (Π, pk) *where* Π *is a public key encryption scheme and* pk *is a public key of* Π *and for any* goal.atk *where* goal.atk *is a security notion such that* goal *is harder than* ind *and* atk *is stronger than* pca *(and thus, may be stronger than or even incomparable with respect to* cca*), if* (Π, pk) *is* goal.atk *secure, for all* α $(0 < \alpha \leq 1)$*, it is impossible to construct even any* α*-weak FKBB reduction* R *such that* $\mathcal{A}_{\mathsf{goal.atk}[\Pi,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{ind.cca}[\Pi,pk]}$.

REFERENCES

1. Canetti R. Universally composable security:a new paradigm for cryptographic protocols. In *IEEE Symposium on Foundations of Computer Science – FOCS 2001*. IEEE Computer Society: Las Vegas, Nevada, USA, 2001; 136–145.
2. Canetti R, Krawczyk H, Nielsen J. Relaxing chosen-ciphertext security. In *Advances in Cryptology – CRYPTO 2003*. Springer: Santa Barbara, California, USA, 2003; 565–582.
3. Ajtai M, Dwork C. A public-key cryptosystem with worst-case/average-case equivalence. In *ACM Symposium on Theory of Computing – STOC 1997*. ACM: El Paso, Texas, USA, 1997; 284–293.
4. Peikert C, Waters B. Lossy trapdoor functions and their applications. In *ACM Symposium on Theory of Computing – STOC 2008*. ACM: Victoria, British Columbia, Canada, 2008; 187–196.
5. Rogaway P. Formalizing human ignorance. In *Progress in Cryptology- VIETCRYPT 2006*, 2006; 211–228.
6. Goldwasser S, Micali S, Rivest R. A digital signature scheme against adaptive chosen message attack. *SIAM Journal on Computing* 1988; **17**(2): 281–308.
7. Håstad J, Impagliazzo R, Levin LA, Luby M. A pseudorandom generator from any one-way function. *SIAM Journal on Computing* 1999; **28**(4): 1364–1396.
8. Goldreich O, Goldwasser S, Micali S. How to construct random functions. *Journal of the ACM* 1986; **33**(4): 792–807.
9. Rompel J. One-way functions are necessary and sufficient for secure signatures. In *ACM Symposium on Theory of Computing – STOC 1990*. ACM: Baltimore, Maryland, USA, 1990; 387–394.
10. Naor M. Bit commitment using pseudorandomness. *Journal of Cryptology* 1991; **4**(2): 151–158.
11. Goldreich O, Micali S, Wigderson A. Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. *Journal of the ACM* 1991; **38**(3): 690–728.
12. Impagliazzo R, Rudich S. Limits on the provable consequences of one-way permutations. In *Advances in Cryptology – CRYPTO 1988*. Springer: Santa Barbara, California, USA, 1988; 8–26.
13. Simon DR. Finding collisions on a one-way street: Can secure hash functions be based on general assumptions? In *Advances in Cryptology - EUROCRYPT 1998*. Springer: Espoo, Finland, 1998; 334–345.
14. Gertner Y, Kannan S, Malkin T, Reingold O, Viswanathan M. The relationship between public key encryption and oblivious transfer. In *IEEE Symposium on Foundations of Computer Science – FOCS 2000*. IEEE Computer Society: Redondo Beach, California, 2000; 325–335.
15. Gertner Y, Malkin T, Reingold O. On the impossibility of basing trapdoor functions on trapdoor predicates. In *IEEE Symposium on Foundations of Computer Science – FOCS 2001*. IEEE Computer Society: Las Vegas, Nevada, USA, 2001; 126–135.
16. Reingold O, Trevisan L, Vadhan S. Notions of reducibility between cryptographic primitives. In *Theory of Cryptography – TCC 2004*, Vol. 2951. Springer: Cambridge, MA, USA, 2004; 1–20.
17. Kim JH, Simon DR, Tetali P. Limits on the efficiency of one-way permutation-based hash functions. In *IEEE Symposium on Foundations of Computer Science – FOCS 1999*. IEEE Computer Society: New York, NY, USA, 1999; 535–542.
18. Gennaro R, Trevisan L. Lower bounds on the efficiency of generic cryptographic constructions. In *IEEE Symposium on Foundations of Computer Science – FOCS 2000*. IEEE Computer Society: Redondo Beach, California, USA, 2000; 305–313.
19. Gennaro R, Gertner Y, Katz J. Lower bounds on the efficiency of encryption and digital signature schemes. In *ACM Symposium on Theory of Computing – STOC 2003*. ACM: San Diego, CA, USA, 2003; 417–425.
20. Paillier P, Vergnaud D. Discrete-log-based signatures may not be equivalent to discrete log. In *Advances in Cryptology – ASIACRYPT 2005*, Vol. 3788. Springer: Chennai, India, 2005; 1–20.

21. Paillier P, Villar JL. Trading one-way against chosen-ciphertext security in factoring-based encryption. In *Advances in Cryptology – ASIACRYPT 2006*, Vol. 4284. Springer: Shanghai, China, 2006; 252–266.
22. Paillier P. Impossibility proof for RSA signatures in the standard model. In *Progress in Cryptology – CT-RSA 2007*, Vol. 4377. Springer: San Francisco, CA, USA, 2007; 31–48.
23. Fischlin M, Schroder D. On the impossibility of three-move blind signature schemes. In *Advances in Cryptology - EUROCRYPT 2010*, Vol. 6110. Springer: French Riviera, 2010; 197–215.
24. Pass R. Limits of provable security from standard assumptions. In *STOC 2011*. ACM: San Jose, CA, USA, 2011; 109–118.
25. Gentry C, Wichs D. Separating succinct non-interactive arguments from all falsifiable assumptions. In *STOC 2011*. ACM: San Jose, CA, USA, 2011; 99–108.
26. Abe M, Groth J, Ohkubo M. Separating short structure-preserving signatures from non-interactive assumptions. In *Advances in Cryptology – ASIACRYPT 2011*, Vol. 7073. Springer: Seoul, South Korea, 2011; 628–646.
27. Hofheinz D, Jager T, Knapp E. Waters signatures with optimal security reduction. In *Public Key Cryptography 2012*, Vol. 7293. Springer: Darmstadt, Germany, 2012; 66–83.
28. Wichs D. Barriers in cryptography with weak, correlated and leaky sources. In *ITCS 2013*. ACM: Berkeley, CA, USA, 2013; 111–126.
29. Fischlin M, Fleischhacker N. Limitations of the meta-reduction technique: the case of schnorr signatures. In *Advances in Cryptology – EUROCRYPT 2013*, Vol. 7881. Springer: Athens, Greece, 2013; 444–460.
30. Baldimtsi F, Lysyanskaya A. On the security of one-witness blind signature schemes. In *Advances in Cryptology – ASIACRYPT 2013*, Vol. 8270. Springer: Bengaluru, India, 2013; 82–99.
31. Lewko AB, Waters B. Why proving hibe systems secure is difficult. In *Advances in Cryptology – EUROCRYPT 2014*, Vol. 8441. Springer: Copenhagen, Denmark, 2014; 58–76.
32. Zhang J, Zhang Z, Chen Y, Guo Y, Zhang Z. Black-box separations for one-more (static) cdh and its generalization. In *Advances in Cryptology – ASIACRYPT 2014*, Vol. 8874. Springer: Kaoshiung, Taiwan, 2014; 366–385.
33. Bernhard D, Fischlin M, Warinschi B. Adaptive proofs of knowledge in the random oracle model. In *Public Key Cryptography 2015*, Vol. 9020. Springer: Gaithersburg, MD, USA, 2015; 629–649.
34. Fischlin M. Black-box reductions and separations in cryptography. In *AFRICACRYPT 2012*, Vol. 7374. Springer: Ifrance, Morocco, 2012; 413–422.
35. Dolev D, Dwork C, Naor M. Non-malleable cryptography. In *ACM Symposium on Theory of Computing – STOC 1991*. ACM: New Orleans, Louisiana, 1991; 542–552.
36. Bellare M, Desai A, Pointcheval D, Rogaway P. Relations among notions of security for public-key encryption schemes. In *Advances in Cryptology – CRYPTO 1998*, Vol. 1462. Springer: Santa Barbara, California, USA, 1998; 26–45.
37. Okamoto T, Pointcheval D. REACT: Rapid enhanced-security asymmetric cryptosystem transform. In *Progress in Cryptology – CT-RSA 2001*, Vol. 2020. Springer: San Francisco, CA, USA, 2001; 159–174.

APPENDIX A: TABLES FOR SUMMARIZING OUR IMPOSSIBILITY RESULTS

Table I. Impossibility results on fixed key black-box reductions for digital signatures, where each cell indicates whether for security notion **goal.atk**, which is determined by the vertical and horizontal terms, it is (im)possible to construct any fixed key black-box (FKBB) reduction from a fixed key **goal.atk** adversary to a fixed key **euf.cma** adversary or not.

	goal → euf goal → uuf	goal → euf uuf → goal	goal → euf atk ↛ uuf	euf → goal uuf ↛ goal	euf → goal uuf ↔ goal	uuf → goal euf ↛ goal
atk → cma atk → kma	Theorem 1	Theorem 1 and 2	Theorem 1	?	Theorem 2	Theorem 2
atk → cma atk → kma	Theorem 1 and 3	Theorem 1, 2 ,and 3	Theorem 1 and 3	?	Theorem 2	Theorem 2
atk → cma atk → kma	Theorem 1	Theorem 1 and 2	Theorem 1	?	Theorem 2	Theorem 2
cma → atk atk ↛ kma	?	?	?	trivial	trivial	?
cma → atk atk ↔ kma	Theorem 3	Theorem 3	Theorem 3	trivial	trivial	?
cma ↛ atk kma → atk	Theorem 3	Theorem 3	Theorem 3	?	?	?

Specifically, "Theorem X (and Y)" means that any FKBB reduction is proven impossible because of Theorem X (and Y); "trivial" means that FKBB reductions can be always trivially constructed, and "?" means that it has been still not proven whether FKBB reductions can be constructed or not. The conditions, which the vertical and horizontal terms determine, are described by using the following notations: **goal**1 → **goal**2 denotes that **goal**1 is harder than **goal**2; **atk**1 → **atk**2 denotes that **atk**1 is weaker than **atk**2, and **goal**1/**atk**1 ↔ **goal**2/**atk**2 denotes that **goal**1/**atk**1 is comparable with respect to **goal**2/**atk**2. And **goal**1/**atk**1 ↛ **goal**2/**atk**2 denotes that **goal**1/**atk**1 is not comparable with respect to **goal**2/**atk**2 (**Definition 6**). cma, chosen message attack; kma, known message attack; atk, attack model; uuf, universal unforgery; goal, adversarial goal; euf, existential unforgery.

Table II. Impossibility results on FKBB reductions for public key encryption schemes, where each cell indicates whether for security notion **goal.atk**, which is determined by the vertical and horizontal terms, it is (im)possible to construct any FKBB reduction from a fixed key **goal.atk** adversary to a fixed key **euf.cma** adversary or not.

	goal → ind goal → ow	goal → ind ow → goal	goal → ind atk ↛ ow	ind → goal ow ↛ goal	ind → goal ow ↔ goal	ow → goal ind ↛ goal
atk → cca atk → pca	Theorem 4	Theorem 4 and 5	Theorem 4	?	Theorem 5	Theorem 5
atk → cca atk → pca	Theorem 4 and 6	Theorem 4, 5, and 6	Theorem 4 and 6	?	Theorem 5	Theorem 5
atk → cca atk → pca	Theorem 4	Theorem 4 and 5	Theorem 4	?	Theorem 5	Theorem 5
cca → atk atk ↛ pca	?	?	?	trivial	trivial	?
cca → atk atk ↔ pca	Theorem 6	Theorem 6	Theorem 6	trivial	trivial	?
cca ↛ atk pca → atk	Theorem 6	Theorem 6	Theorem 6	?	?	?

Specifically, "Theorem X (and Y)" means that any FKBB reduction is proven impossible due to Theorem X (and Y), "trivial" means that FKBB reductions can be always trivially constructed, and "?" means that it has been still not proven whether FKBB reductions can be constructed or not. The conditions, which the vertical and horizontal terms determine, are described by using the following notations: **goal**1 → **goal**2 denotes that **goal**1 is harder than **goal**2, and **atk**1 → **atk**2 denotes that **atk**1 is weaker than **atk**2; **goal**1/**atk**1 ↔ **goal**2/**atk**2 denotes that **goal**1/**atk**1 is comparable with respect to **goal**2/**atk**2, and **goal**1/**atk**1 ↛ **goal**2/**atk**2 denotes that **goal**1/**atk**1 is not comparable with respect to **goal**2/**atk**2 (**Definition 6**). goal, adversarial goal; atk, attack model; pca, plaintext checking attack; cca, chosen ciphertext attack; ind, indistinguishability; ow, one-wayness.

APPENDIX B: PROOFS OF IMPOSSIBILITY OF FKBB REDUCTION FOR PUBLIC KEY ENCRYPTION

B.1 Proof of Theorem 4

For proving the theorem, we first address the following lemma.

Lemma 3. *For all* (Π, pk) *and* atk*, if* (Π, pk) *is* ind.atk *secure, for all* α $(0 < \alpha \leq 1)$*, it is impossible to construct any* α*-weak FKBB reduction* R' *such that* $\mathcal{A}_{\mathsf{ind.atk}[\Pi,pk]} \Leftarrow_{R'} \mathcal{A}_{\alpha\text{–}\mathsf{ind.cca}[\Pi,pk]}$.

Proof. Towards a contradiction, we assume that an α-weak implementation of an FKBB R such that $\mathcal{A}_{\mathsf{ind.atk}[\Pi,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{ind.cca}[\Pi,pk]}$ is given. Then, the theorem is proven by constructing a real-life Algorithm B, which breaks (Π, pk) in the sense of ind.atk.

We can construct such B by using R as follows. B first picks two random plaintexts m_0 and m_1, and is given a ciphertext c_b, which is encryption of either m_0 or m_1. B next activates R, and then, R starts interacting with a (virtual) oracle $\mathcal{O}_{\mathsf{atk}}$ (which is determined by atk) and a (virtual) α-strong fixed key ind.cca adversary on (Π, pk). When R submits a query to the virtual $\mathcal{O}_{\mathsf{atk}}$, B responds to it in such a way that B submits the same query to his own $\mathcal{O}_{\mathsf{atk}}$ and returns the answer from $\mathcal{O}_{\mathsf{atk}}$ as it is. On the other hand, B does not need to simulate the α-strong fixed key ind.cca adversary until R correctly answers to all queries from B who pretends as the α-strong fixed key ind.cca adversary. Therefore, R's view is perfectly indistinguishable from the normal communication with $\mathcal{O}_{\mathsf{atk}}$ and an α-strong fixed key ind.cca adversary.

Because for all $A \in \mathcal{A}_{\alpha\text{–}\mathsf{ind.cca}[\Pi,pk]}$, R^A breaks (Π, pk) in the sense of ind.atk, but R itself cannot ((if it can, this contradicts to the assumption that (Π, pk) is goal.atk secure)); it is guaranteed that R correctly answers to all queries from B with probability more than P_{min}. This implies that by submitting c_b to R, B can obtain decryption of it with probability more than P_{min}. We note that (1) c_b is not prohibited to submit to the decryption oracle which R simulates, and (2) from R's view, c_b merely a ciphertext of a random plaintext. Therefore, R always treats c_b in the same way as other normal decryption queries. Hence, B can obtain the underlying plaintext of c_b with probability more than P_{min}, and in the case that it cannot, B outputs a random bit. Then, B correctly guesses the underlying plaintext of c_b with probability more than $1/2 \cdot P_{min} + 1/2 (= P_{min} + 1/2(1 - P_{min}))$. We can also confirm that B is a real-life adversary in a similar manner to Lemma 1.

Therefore, B works as a successful fixed key ind.atk adversary, and it can be explicitly constructed if we are given any implementation of R such that $\mathcal{A}_{\mathsf{ind.atk}[\Pi,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{ind.cca}[\Pi,pk]}$, and this contradicts to the assumption that (Π, pk) is ind.atk secure. □

Next, we address the following lemma which can be trivially proven by definition.

Lemma 4. *For all* (Π, pk) *and* goal.atk *such that* goal *is harder than* ind*, it is always possible to construct a fixed key black-box reduction* R *such that* $\mathcal{A}_{\mathsf{ind.atk}[\Pi,pk]} \Leftarrow_R \mathcal{A}_{\mathsf{goal.atk}[\Pi,pk]}$.

Becuase of Lemma 4, it is guaranteed that an FKBB R' such that $\mathcal{A}_{\mathsf{ind.atk}[\Pi,pk]} \Leftarrow_{R'} \mathcal{A}_{\mathsf{goal.atk}[\Pi,pk]}$ can be explicitly constructed. Therefore, if an α-weak FKBB reduction R such that $\mathcal{A}_{\mathsf{goal.atk}[\Pi,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{ind.cca}[\Pi,pk]}$ can be constructed, then by transitivity, another α-weak FKBB reduction $R'' = R \circ R'$ such that $\mathcal{A}_{\mathsf{ind.atk}[\Pi,pk]} \Leftarrow_{R''} \mathcal{A}_{\alpha\text{–}\mathsf{ind.cca}[\Pi,pk]}$ can be always constructed as well. Furthermore, assuming that an implementation of such an R is given, (Π, pk) is ind.cca secure if (Π, pk) is goal.atk secure, and this implies that (Π, pk) is ind.atk secure if (Π, pk) is goal.atk secure because atk is weaker than cca. However, because of Lemma 3, it is shown to be impossible to construct such R'' if (Π, pk) is ind.atk secure, and thus, R cannot be constructed neither, which proves the theorem.

B.2 Proof of Theorem 5

This theorem can be proven in a similar manner to Lemma 3. We assume that an implementation of an α-weak FKBB R such that $\mathcal{A}_{\mathsf{goal.atk}[\Pi,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{ind.cca}[\Pi,pk]}$ is given. Then, the theorem is proven by constructing a real-life adversary B, which breaks (Π, pk) in the sense of ow.atk (not goal.atk). Namely, if B is an implementation of a fixed key ow.atk adversary on (Π, pk), then by using B, it is also possible to construct a fixed key ow.atk adversary on (Π, pk) for all goal such that goal is easier than ow.

For given c^*, B first activates R, and then, R starts interacting with a (virtual) oracle $\mathcal{O}_{\mathsf{atk}}$ (which is determined by atk) and a (virtual) α-strong fixed key ind.cca adversary on (Π, pk). When R submits a query to the virtual $\mathcal{O}_{\mathsf{atk}}$, B responds to it in such a way that B submits the same query to his own $\mathcal{O}_{\mathsf{atk}}$, and returns the answer from $\mathcal{O}_{\mathsf{atk}}$ as it is. On the other hand, B does not need to simulate the α-strong fixed key ind.cca adversary until R correctly answers to all queries from B who pretends as the α-strong fixed key ind.cca adversary. Therefore, R's view is perfectly indistinguishable from the normal communication with $\mathcal{O}_{\mathsf{atk}}$ and an α-strong fixed key ind.cca adversary.

Because for all $A \in \mathcal{A}_{\alpha\text{–}\mathsf{ind.cca}[\Pi,pk]}$, R^A breaks (Π, pk) in the sense of goal.atk, but R itself cannot (if it can, this contradicts to the assumption that (Π, pk) is goal.atk secure), it is guaranteed that R correctly answers to all queries from B with probability more than P_{min}. This implies that by submitting c^* to R, B can obtain decryption of it (i.e., m^*) with probability more than P_{min}. We note that R always treats c^* in the same way as other normal decryption queries. Hence, B can obtain m^* with probability more than P_{min}. We can also confirm that B is a real-life adversary in a similar manner to Lemma 1.

Therefore, B works as a successful fixed key ow.atk adversary, and it can be explicitly constructed if we are given any implementation of R such that $\mathcal{A}_{\mathsf{euf.atk}[\Pi,pk]} \Leftarrow_R \mathcal{A}_{\mathsf{euf.cma}[\Pi,pk]}$, which contradicts to the assumption that (Π, pk) is goal.atk secure (since goal is easier than ow).

B.3 Proof of Theorem 6

We assume that an implementation of an α-weak FKBB R such that $\mathcal{A}_{\mathsf{goal.atk}[\Pi,pk]} \Leftarrow_R \mathcal{A}_{\alpha\text{–}\mathsf{ind.cca}[\Pi,pk]}$ is given. Then, the theorem is proven by constructing a real-life adversary B, which breaks (Π, pk) in the sense of goal.atk. Let (C, P_c, x, y) be the constant value, the probability of succeeding in the attack by random guess, the correct output, and the input to the adversary, which are determined by atk (see Definition 2 for details).

B activates R and inputs y to R. Then, R starts interacting with a (virtual) oracle $\mathcal{O}_{\mathsf{atk}}$ (which is determined by atk) and a (virtual) α-strong fixed key ind.cca adversary on (Π, pk). When R submits a query to the virtual $\mathcal{O}_{\mathsf{atk}}$, B responds to it in such a way that B submits the same query to his own $\mathcal{O}_{\mathsf{atk}}$ and returns the answer from $\mathcal{O}_{\mathsf{atk}}$ as it is. On the other hand, B does not need to simulate the α-strong fixed key ind.cca adversary until R correctly answers to all queries from B who pretends as the ind.cca adversary. Therefore, R's view is perfectly indistinguishable from the normal communication with $\mathcal{O}_{\mathsf{atk}}$ and an α-strong fixed key ind.cca adversary.

At some point, B (who is simulating an α-strong fixed key ind.cca adversary) is enforced to commit two plaintexts m_0 and m_1, which will be challenged, and R returns the challenge ciphertext $\tilde{c}_b$. Furthermore, at another point, it is again enforced to outputs the correct guess on the underlying plaintext of $\tilde{c}_b$.

Then, B invokes an FKBB reduction $\overline{R}$ such that $\mathcal{A}_{\mathsf{goal.atk}[\Pi,pk]} \Leftarrow_{\overline{R}} \mathcal{A}_{\mathsf{goal.pca}[\Sigma,pk]}$. Because atk is stronger than pca, such an $\overline{R}$ can be always constructed. B next activates $\overline{R}$, and then, $\overline{R}$ starts interacting with a (virtual) oracle $\mathcal{O}_{\mathsf{atk}}$ and a (virtual) fixed key goal.pca adversary on (Π, pk). When $\overline{R}$ submits a query to the virtual $\mathcal{O}_{\mathsf{atk}}$, B responds to it by interacting with his own $\mathcal{O}_{\mathsf{atk}}$. On the other hand, B does not need to simulate the goal.pca adversary until $\overline{R}$ correctly answers to all queries. We note that $\overline{R}$'s view is perfectly indistinguishable from the normal communication with $\mathcal{O}_{\mathsf{atk}}$ and an goal.pca adversary.

Similarly to the proof of Lemma 1, we see that B works as a fixed key goal.atk adversary, which contradicts to the assumption that (Π, pk) is goal.atk secure.