The intention of the document is to clarify differences between different security notions on searchable encryption. For simplicity, we consider static security (i.e. without queries), but it can be easily generalised to include queries. There are two 'parameters' in the definitions, namely if the adversary is a bit adversary or a string adversary, and if the notion we consider is black-box or non-black-box. We begin by defining the security notions.

Definition 1 (Semantic Security Notion for Bit Adversaries)**.** *Consider the following game.*

```
$Real_{\mathcal{A}}(n)$
    $k \leftarrow_{\$} \mathsf{KGen}(1^n)$
    $(db, \boldsymbol{st}_{\mathcal{A}}) \leftarrow \mathcal{A}_0(1^n)$
    $edb, \leftarrow \mathsf{Enc}(1^n, k, db)$
    $b \leftarrow \mathcal{A}_1(1^n, edb, \boldsymbol{st}_{\mathcal{A}})$
    return $b$
```

```
$\mathsf{Sim}_{\mathcal{A},\mathcal{S}}(n)$
    $k \leftarrow_{\$} \mathsf{KGen}(1^n)$
    $(db, \boldsymbol{st}_{\mathcal{A}}) \leftarrow \mathcal{A}_0(1^n)$
    $l \leftarrow \mathcal{L}_{\mathcal{M}}(1^n, db)$
    $edb \leftarrow \mathcal{S}(1^n, l)$
    $b \leftarrow \mathcal{A}_1(1^n, edb, \boldsymbol{st}_{\mathcal{A}})$
    return $b$
```

We say that the underlying searchable encryption scheme is $\mathcal{L}_{\mathcal{M}}$-semantic secure in the black-box model for bit adversary if there exists a simulator $\mathcal{S}$ such that for all PPT adversaries $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ where $\mathcal{A}_1$ outputs a bit,

$$\Pr[Real_{\mathcal{A}}(n) = 1] - \Pr[\mathsf{Sim}_{\mathcal{A},\mathcal{S}}(n) = 1] \leq \mathsf{negl}(n)\,. \tag{1}$$

We say that the underlying searchable encryption scheme is $\mathcal{L}_{\mathcal{M}}$-semantic secure in the non-black-box model for bit adversary if for all PPT adversaries $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ where $\mathcal{A}_1$ outputs a bit, there exists a simulator $\mathcal{S}$ such that,

$$\Pr[Real_{\mathcal{A}}(n) = 1] - \Pr[\mathsf{Sim}_{\mathcal{A},\mathcal{S}}(n) = 1] \leq \mathsf{negl}(n)\,. \tag{2}$$

Definition 2 (Semantic Security Notion for String Adversaries)**.** *Consider the following game.*

```
$Real_{\mathcal{A}}(n)$
    $k \leftarrow_{\$} \mathsf{KGen}(1^n)$
    $(db, \boldsymbol{st}_{\mathcal{A}}) \leftarrow \mathcal{A}_0(1^n)$
    $edb, \leftarrow \mathsf{Enc}(1^n, k, db)$
    $s \leftarrow \mathcal{A}_1(1^n, edb, \boldsymbol{st}_{\mathcal{A}})$
    return $s$
```

```
$\mathsf{Sim}_{\mathcal{A},\mathcal{S}}(n)$
    $k \leftarrow_{\$} \mathsf{KGen}(1^n)$
    $(db, \boldsymbol{st}_{\mathcal{A}}) \leftarrow \mathcal{A}_0(1^n)$
    $l \leftarrow \mathcal{L}_{\mathcal{M}}(1^n, db)$
    $edb \leftarrow \mathcal{S}(1^n, l)$
    $s \leftarrow \mathcal{A}_1(1^n, edb, \boldsymbol{st}_{\mathcal{A}})$
    return $s$
```

We say that the underlying searchable encryption scheme is $\mathcal{L}_{\mathcal{M}}$-semantic secure in the black-box model for string adversary if there exists a simulator $\mathcal{S}$ such that for all PPT adversaries $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$, for all PPT distinguishers $\mathcal{D}$,

$$\Pr[\mathcal{D}(Real_{\mathcal{A}}(n)) = 1] - \Pr[\mathcal{D}(\mathsf{Sim}_{\mathcal{A},\mathcal{S}}(n)) = 1] \leq \mathsf{negl}(n)\,. \tag{3}$$

We say that the underlying searchable encryption scheme is $\mathcal{L}_{\mathcal{M}}$-semantic secure in the non-black-box model for string adversary if for all PPT adversaries $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$, there exists a simulator $\mathcal{S}$, such that for all PPT distinguishers $\mathcal{D}$,

$$\Pr[\mathcal{D}(Real_{\mathcal{A}}(n)) = 1] - \Pr[\mathcal{D}(\mathsf{Sim}_{\mathcal{A},\mathcal{S}}(n)) = 1] \leq \mathsf{negl}(n)\,. \tag{4}$$

For simplicity, we call the four notions **B-BB-SS**, **B-NBB-SS**, **S-BB-SS** and **S-NBB-SS** respectively. We will now present the implications.

$$\begin{tikzcd}
\textbf{B-BB-SS} \arrow[r, shift left] \arrow[d] & \textbf{S-BB-SS} \arrow[l, shift left] \arrow[d] \\
\textbf{B-NBB-SS} & \textbf{S-NBB-SS} \arrow[l]
\end{tikzcd}$$

Figure 1: Implication between notions

To summarise the implications, we have:

1. In the black-box model, bit adversary and string adversary are equally strong.
2. Security in black-box model implies security in non-black-box model.
3. In the non-black-box model, bit adversary and string adversary are not equivalent.

We will now give a proof of the implications.

Proof. To begin with, we show that security in black-box model implies security in non-black-box model. Suppose there is a bit adversary in the black-box model, then this adversary works for all simulators, hence by using this adversary in the non-black box model, he wins with probability equal to the amount he wins in the black-box model. Hence for bit adversaries, security in black-box model implies security in non-black-box model. We use a very similar argument for string adversaries, the only difference is that we use the $(\mathcal{A}, \mathcal{D})$ that breaks the security in the black-box model to break security in the non-black-box model.

Since bit adversary is a special type of string adversary, we have implications from string adversary to bit adversary for free. It remains to show that in the black-box model, security against bit adversary implies security against string adversary. Suppose that the scheme is not secure against string adversary, then for all simulators, there exists an adversary $\mathcal{A}$ such that there is a distinguisher $\mathcal{D}$ wining the security game with non-negligible probability. The bit adversary can be easily constructed by composing $\mathcal{A}$ and $\mathcal{D}$, i.e. we run the two adversaries one after another and returns the bit from $\mathcal{D}$ as the answer of the bit adversary. The bit adversary wins with probability equal to that of the corresponding string adversary. □