1 Rivest (1997)

1.1 Original Definition

The original definition of Rivest looks like this:

Consider a function f that takes the message sequence $m_1, m_2 \dots m_s$ and returns pseudo-message sequence $m'_1, m'_2 \dots m'_{s'}$. We call f an AONT when the following are satisfied:

- The transformation f is reversible: Given the pseudo-message sequence, one can obtain the original message sequence.
- Both f and its inverse are efficiently computable (PT)
- It is computationally infeasible to compute any function of any message block if any one of the pseudo-message blocks is unknown.

1.2 Formalized Definition

This is my attempt to formalize this definition with concrete security games.

Note that because we are talking in concrete security, I make no comment on efficiency of any of the algorithms

An *All-Or-Nothing-Transform* AONT specifies two algorithms ($\mathsf{AONT.Transform}, \mathsf{AONT.Inverse}$), and a block length $\mathsf{AONT.bl}$. We have that $\mathsf{AONT.Transform} : \{\{0,1\}^{\mathsf{AONT.bl}}\}^* \to \{\{0,1\}^{\mathsf{AONT.bl}}\}^*$. We call the domain of this function "message sequences" and the range "pseudo-message sequences". Then $\mathsf{AONT.Inverse}$ is the inverse of this function, meaning that $\mathsf{AONT.Inverse} : \{\{0,1\}^{\mathsf{AONT.bl}}\}^* \to \{\{0,1\}^{\mathsf{AONT.bl}}\}^*$, a mapping that only needs to be defined on pseudo-message sequences that can be generated by $\mathsf{AONT.Transform}$. $\mathsf{AONT.Transform}$ can (and should) be randomized, while $\mathsf{AONT.Inverse}$ is not randomized.

The correctness condition for AONT is

$$\Pr\left[\,\mathsf{AONT.Inverse}(\mathsf{AONT.Transform}((m_1, m_2 \dots m_s)) = (m_1, m_2, \dots m_s))\,\right] = 1$$

where the probability is taken over all possible message sequences $(m_1, m_2 \dots m_s)$ and all possible randomness of the $\mathsf{AONT.Transform}$ function.

Now we can define the following security game:

$\underline{\mathbf{G}^{\text{ind}}_{\mathsf{AONT}}(A)}$
$b \leftarrow\!\!\$\ \{0,1\}$
$b' \leftarrow\!\!\$\ A^{\text{LR}}$
return $(b = b')$
$\underline{\text{LR}(m^*, n^*, i, j)}$
if
$(|m^*| \neq \mathsf{AONT.bl}) \vee (|n^*| \neq \mathsf{AONT.bl}) \vee (i > j)$
then
return $\perp$
end
for $(x = 1, 2, \ldots j)$ **do**
if $(x \neq i)$ **then**
$m_x \leftarrow\!\!\$\ \{0,1\}^{\mathsf{AONT.bl}}$
$n_x \leftarrow\!\!\$\ \{0,1\}^{\mathsf{AONT.bl}}$
else
$m_x \leftarrow m^*$
$n_x \leftarrow n^*$
end
end
if $b = 0$ **then**
$y \leftarrow\!\!\$\ \mathsf{AONT.Transform}(m_1, m_2 \ldots m_s)$
else
$y \leftarrow\!\!\$\ \mathsf{AONT.Transform}(n_1, n_2 \ldots n_s)$
end
return y

Then we say that the AONT indistinguishability advantage of an A is given by:

$$\mathbf{Adv}^{\text{aont}}_{\mathsf{AONT}}(A) = 2 \cdot \Pr\left[\mathbf{G}^{\text{ind}}_{\mathsf{AONT}}(A)\right] - 1$$

1.3 Package Transform

Rivest provides a construction of an AONT proceeding as follows. It makes use of an arbitrary block cipher, with key of length $\mathsf{AONT.bl}$, $E : \{0,1\}^{\mathsf{AONT.bl}} \times \{0,1\}^{\mathsf{AONT.bl}} \rightarrow \mathsf{AONT.bl}$. I edited this a bit for clarity (with respect to the keys).

No proof is provided as to the security of this scheme. The phrasing of the "informal" proof also seems problematic because it talks about an adversary that is attempting to "compute any message block" instead of any function of any message block, which is not the same as was suggested by the definition.

$\underline{\mathsf{AONT.Transform}(m_1, m_2, \ldots m_s)}$

if $\exists i. |m_i| \neq \mathsf{AONT.bl}$ **then**
  return $\perp$
end
$K \leftarrow\!\!\$\ \{0,1\}^{\mathsf{AONT.bl}}$
$K' \leftarrow\!\!\$\ \{0,1\}^{\mathsf{AONT.bl}}$
$m'_{s+1} \leftarrow K'$
for $i = 1, 2 \ldots s$ **do**
  $m'_i \leftarrow m_i \oplus E(K', \langle i \rangle_{\mathsf{AONT.bl}})$
  $h_i \leftarrow E(K, m'_i \oplus \langle i \rangle_{\mathsf{AONT.bl}})$
  $m'_{s+1} \leftarrow m'_{s+1} \oplus h_i$
end
return $(m'_1, m'_2 \ldots m'_s, m'_{s+1}, K)$

$\underline{\mathsf{AONT.Inverse}(m'_1, m'_2 \ldots m'_{s'})}$

if $(\exists i. |m'_i| \neq \mathsf{AONT.bl}) \vee (s' \leq 2)$ **then**
  return $\perp$
end
$K \leftarrow m'_{s'}$
$K' \leftarrow m'_{s'-1}$
$s \leftarrow s' - 2$
for $(i = 1, 2, \ldots s)$ **do**
  $h_i \leftarrow E(K, m'_i \oplus i)$
  $K' \leftarrow K' \oplus h_i$
end
for $(i = 1, 2, \ldots s)$ **do**
  $m_i \leftarrow E(K', i) \oplus m'_i$
end
return $(m_1, m_2 \ldots m_s)$

2 Boyko (1999)

2.1 Overview and Important Notes

Boyko presents the first formal security notion for AONTs, making some changes to the one implied by Rivest. Some of these choices are justified, and some seem less so.

He proposes notions of secuirty based on both adaptive and non-adaptive models, and both semantic security and indistinguishability based definitions. He doesn't explain why there is a need for so many of these, and which ones imply which ones. I think this is interesting and worth looking at.

Finally, the key contribution of this paper (in my opinion) is showing that OAEP is usable in the package transform proposed by Rivest in order to achieve an AONT. With all of the above in mind, I would like to show explicitly that this construction still provides the security guarantees that Boyko claims, under the security definition of Rivest (which is quoted much more often in literature).

2.2 Commentary on Boyko's critique of Rivest (1997)

Boyko lists two major "problems" with the Rivest definition. To me, while the Rivest definition was not explicitly spelt out in a security game, is intuitive and plenty sufficient to discuss AONTs. Especially since many application papers (like all those I study), use the Rivest definition, there are clear benefits to try to show the rest of Boyko's claims using the Rivest definition.

The first of Boyko's claims is that we would want our AONT to be secure against an adversary that is trying to compute some information about the message as a whole, instead of an adversary that is trying to compute some information about one particular message block. Since the former adversary is more general, Boyko claims it would make for a better definition. Note that the analogous definition suggested by this comment of Boyko's would allow the adversary to pick the entire message instead of picking just one block of the message in the game $\mathbf{G}^{\text{ind}}_{\mathsf{AONT}}$ above. The oracle suggested by Boyko will just skip over the random generation of the other blocks done by LR above, and proceed similarly. Then, consider any adversary A against $\mathbf{G}^{\text{ind}}_{\mathsf{AONT}}$ as defined by Rivest. Notice that we can trivially generate adversary A' against the analogous game suggested by

Boyko's comment here. A' will simply take any pair of blocks queried by A and randomly generate the remaining blocks, before passing it to the Boyko oracle analogous to LR. Therefore, if we have an attack against Rivest's model, we have an attack against Boyko's model. This means that if a scheme is an AONT by Boyko's model, it is also an AONT by Rivest's model. This shows that Boyko's claim is true.

More informally (this was contributed by Igors) an adversary may be able to compute a function about the message has a whole without knowing anything about any particular block (e.g. if the first block is equal to the second block). Therefore, Boyko's definition is stronger.

The second of Boyko's claims is that Rivest's definition does not allow for analysis of the relation between the number of bits of AONT output that the adversary has and the information that is leaked about the input. I find this comment very strange since the whole point of AONTs is that no matter how many bits of information is given to the adversary, so long as there is one block that is not accessible to the adversary, it is still computationally infeasible for the adversary to predict any information about the message sequence better than if he randomly guesses. Boyko's paper suggests that instead of stipulating that there must exist a block that the adversary knows nothing about, that we should consider what the adversary's advantage is with respect to the number of bits that were not leaked. This means studying the advantage of adversaries for varying values of l, where the adversary is given all but l bits of the pseudo-message.

Both of these comments are definitely valid. I believe that Rivest's definition considers the cryptanalysis of AONT in a more traditional sense, where the encrypted data is being stored as blocks, or being communicated over a secure channel as blocks. The adversary would then capture or steal entire blocks of the pseudomessage. However, Boyko's definition encompasses more current forms of cryptanalysis, such as side channel attacks, which may leak partial blocks of data. However, since most papers studying constructions and applications of AONT do make use of Rivest's definition, I think there is value in using Rivest's definition as the standard. In addition, I think that intuitively an "all-or-nothing-transform" should have the security properties suggested by Rivest even if the message sequence and pseudomessage sequence is permuted. In fact, I think that we can show that:

Definition 2.1 *We call a scheme* AONT *a strong-AONT if, for all* $f : \{\{0,1\}^{\mathsf{AONT.bl}}\} \to \{\{0,1\}^{\mathsf{AONT.bl}}\}$ *that define permutations on strings,* $(f \circ \mathsf{AONT.Transform}, \mathsf{AONT.Inverse} \circ f^{-1})$ *is an AONT by Rivest's definition.*

I conjecture that the following is true

Theorem 2.2 *A scheme is secure with respect to Boyko's definition (adaptive indistinguishability), for any leakage up to* $\mathsf{AONT.bl}$ *bits if and only if it is a strong-AONT*

This shows some equivalence between the two definitions.

2.3 Other comments

I don't understand why Boyko feels the need to include both indistinguishability and simulation based security definitions. I think that we can prove which one is a stronger claim and move forward with a limited subset of these.

Boyko does present an important result which is to use OAEP in the design of the package transform algorithm. I would like to give an explicit proof (without making use of Boyko's definition) that this still works with Rivest's definition.