1 Syntax

An *All-Or-Nothing-Transform* AONT specifies two algorithms $(\mathsf{AONT.Transform}, \mathsf{AONT.Inverse})$, and a block length $\mathsf{AONT.bl}$. Then, we can associate with AONT a domain and range, $\mathsf{AONT}.\mathcal{D}, \mathsf{AONT}.\mathcal{R} \subset \{\{0,1\}^{\mathsf{AONT.bl}}\}^*$(the set of strings having length that is a multiple of $\mathsf{AONT.bl}$). We call the domain the "message sequences" and the range the "pseudo-message sequences". Then, we have that $\mathsf{AONT.Transform} : \mathsf{AONT}.\mathcal{D} \to \mathsf{AONT}.\mathcal{R}$, a randomized algorithm, and $\mathsf{AONT.Inverse} : \mathsf{AONT}.\mathcal{R} \to \mathsf{AONT}.\mathcal{D}$, a deterministic algorithm.

2 Correctness

The correctness condition for AONT is

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

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

3 Rivest (1997)

$\underline{\mathbf{G}^{\mathrm{ind}}_{\mathsf{AONT}}(A)}$
$b \xleftarrow{\$} \{0,1\}$
$b' \xleftarrow{\$} A^{\mathrm{LR}}$
return $(b = b')$
$\underline{\mathrm{LR}(M, N, i)}$
if $|M| \neq |N|$ **then**
  return $\perp$
end
$(m_1, m_2 \ldots m_s) \leftarrow M$
$(n_1, n_2 \ldots n_s) \leftarrow N$
$n_i \leftarrow \epsilon$
$m_i \leftarrow \epsilon$
if $b = 0$ **then**
  $y \xleftarrow{\$} \mathsf{AONT.Transform}(m_1, m_2 \ldots m_s)$
else
  $y \xleftarrow{\$} \mathsf{AONT.Transform}(n_1, n_2 \ldots n_s)$
end
return y

Then we say that the indistinguishability adversary A has l-AONT-IND advantage:

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

4 Boyko (1999)/ Canetti et. al (2000)

$\underline{\mathbf{G}^{\text{leak}}_{\mathsf{AONT},l}(A)}$

$b \leftarrow\!\!\$\ \{0,1\}$
$b' \leftarrow\!\!\$\ A^{\text{LR}}$
return $(b = b')$

$\underline{\text{LR}(M, N, S)}$

if $|M| \neq |N|$ **then**
  return $\perp$
end
$(m_1, m_2 \ldots m_s) \leftarrow M$
$(n_1, n_2 \ldots n_s) \leftarrow N$
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
if $(|S| \neq |y|) \vee (\mathsf{Hamm}(S) > (|y| - l))$ **then**
  return $\perp$
else
  $y \leftarrow y \,\&\, S$
end
return y

Note that $|M|$ is the length of the string M in bits, & is a bitwise AND and $\mathsf{Hamm}(M)$ *takes the hamming weight of M*

Then we say that the leakage adversary A has l-AONT-LEAK advantage:

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

5 Leakage Resilience Model

$\underline{\mathbf{G}^{\mathrm{lr}}_{\mathsf{AONT},m}(A)}$
$b \leftarrow\!\!\$\ \{0,1\}$
$b' \leftarrow\!\!\$\ A^{\mathrm{LR}}$
return $(b = b')$
$\underline{\mathrm{LR}(M,N,C)}$
if $|M| \neq |N|$ **then**
  return $\perp$
end
$(m_1, m_2 \ldots m_s) \leftarrow M$
$(n_1, n_2 \ldots n_s) \leftarrow N$
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
if $(C \notin \mathcal{C}_{|y|,(|y|-m)})$ **then**
  return $\perp$
else
  return $C(y)$
end

Note that $\mathcal{C}_{n,m}$ is the set of boolean circuits taking n inputs and m outputs, expressed in a string in some reasonable encoding. Then, for $C \in \mathcal{C}_{n,m}$, when we run $C(S)$ for some binary string S of length n, C will take as input the bits of S and return a m bit long string.

Then we say that the leakage resilience adversary A has m-AONT-LR advantage:

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

6 Relationship between Notions

6.1 $\mathsf{AONT.bl} - \mathsf{AONT} - \mathsf{L} \implies \mathsf{AONT} - \mathsf{IND}$

Theorem 6.1 *For any* $\mathsf{AONT} - \mathsf{IND}$ *adversary A, we can construct* $\mathsf{AONT.bl} - \mathsf{AONT} - \mathsf{L}$ *adversary B, running in the same time and making the same number of queries, such that*

$$\boldsymbol{Adv}^{\textit{aont-ind}}_{\mathsf{AONT}}(A) \leq \boldsymbol{Adv}^{\textit{aont-leak}}_{\mathsf{AONT},\mathsf{AONT.bl}}(B)$$

Here is the adversary (the full proof is omitted for now):

$\underline{B^{\mathrm{LR}}}$
    $b \leftarrow\!\!\$\ A^{\textsc{SimLR}}$
    return b
$\underline{\textsc{SimLR}(M, N, i)}$
    $mask \leftarrow \epsilon$
    $s \leftarrow \lceil \frac{|M|}{\mathsf{AONT.bl}} \rceil$
    for $j = 1, 2, \ldots s$ **do**
        if $j \neq i$ **then**
            $mask \leftarrow mask || 1^{\mathsf{AONT.bl}}$
        else
            $mask \leftarrow mask || 0^{\mathsf{AONT.bl}}$
        end
    end
    return $\mathrm{LR}(M, N, mask)$

6.2 $l-\mathsf{AONT}-\mathsf{L} \implies l-\mathsf{AONT}-\mathsf{LR}$

Theorem 6.2 *For any $l-\mathsf{AONT}-\mathsf{L}$ adversary A, we can construct $l-\mathsf{AONT}-\mathsf{LR}$ adversary B, running in the same time and making the same number of queries, such that*

$$\boldsymbol{Adv}^{\textit{aont-leak}}_{\mathsf{AONT},l}(A) \leq \boldsymbol{Adv}^{\textit{aont-lr}}_{\mathsf{AONT},l}(B)$$

Here is the adversary (the full proof is omitted for now):

$\underline{B^{\mathrm{LR}}}$
    $b \leftarrow\!\!\$\ A^{\textsc{SimLR}}$
    return b
$\underline{\textsc{SimLR}(M, N, mask)}$
    return $\mathrm{LR}(M, N, C_{mask})$
$\underline{C_{mask}(X)}$
    return $mask\ \&\ X$

6.3 $\mathsf{AONT.bl}-\mathsf{AONT}-\mathsf{L} \not\Rightarrow \mathsf{AONT.bl}-\mathsf{AONT}-\mathsf{LR}$

Consider the following AONT scheme, Checksum, which is defined for all choices of Checksum.bl. It has $\mathsf{Checksum}.\mathcal{D} = \{0,1\}^{\mathsf{Checksum.bl}}$ and $\mathsf{Checksum}.\mathcal{R} = \{0,1\}^{\mathsf{Checksum.bl}^2}$:

$\underline{\mathsf{Checksum.Transform}(m)}$	$\underline{\mathsf{Checksum.Inverse}(m'_1, m'_2 \ldots m'_{\mathsf{Checksum.bl}})}$
$m'_{\mathsf{Checksum.bl}} \leftarrow m$	$m \leftarrow m'_{\mathsf{Checksum.bl}}$
for $i = 1, 2, \ldots \mathsf{Checksum.bl} - 1$ **do**	**for** $i = 1, 2, \ldots \mathsf{Checksum.bl} - 1$ **do**
$m'_i \leftarrow\!\!\$\ \{0,1\}^{\mathsf{Checksum.bl}}$	$m \leftarrow m'_i \oplus m$
$m'_{\mathsf{Checksum.bl}} \leftarrow m'_i \oplus m'_{\mathsf{Checksum.bl}}$	**end**
end	**return** m
return $(m'_1, m'_2 \ldots m'_{\mathsf{Checksum.bl}})$	

First, let's show that $\mathsf{Checksum}$ is $\mathsf{Checksum.bl} - \mathsf{AONT} - \mathsf{L}$ secure.

Next, we can provide a $\mathsf{Checksum.bl} - \mathsf{AONT} - \mathsf{LR}$ adversary A.

6.4 $\mathsf{AONT} - \mathsf{IND} \not\Rightarrow \mathsf{AONT.bl} - \mathsf{AONT} - \mathsf{L}$

Rivest provides a construction of an AONT known as the package transform. It makes use of an arbitrary block cipher, with key of length $\mathsf{AONT.bl}$, $E : \{0,1\}^{\mathsf{AONT.bl}} \times \{0,1\}^{\mathsf{AONT.bl}} \to \mathsf{AONT.bl}$.

I modified this scheme slightly to achieve a scheme that is $\mathsf{AONT} - \mathsf{IND}$ secure but not $\mathsf{AONT.bl} - \mathsf{AONT} - \mathsf{L}$ secure.

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

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
$m'_{s+1} \leftarrow E(K, m'_{s+1})$
$m'_{s+2} \leftarrow m'_{s+1}\ \&\ 1^{\frac{\mathsf{AONT.bl}}{2}} 0^{\frac{\mathsf{AONT.bl}}{2}}$
$m'_{s+1} \leftarrow m'_{s+1}\ \&\ 0^{\frac{\mathsf{AONT.bl}}{2}} 1^{\frac{\mathsf{AONT.bl}}{2}}$
return $(m'_1, m'_2 \ldots m'_s, m'_{s+1}, m'_{s+2}, K)$

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

if $(\exists i. |m'_i| \neq \mathsf{AONT.bl}) \vee (s' \leq 2)$ **then**
  return $\perp$
end
$K \leftarrow m'_{s'}$
$K' \leftarrow E^{-1}(K, m'_{s'-1} \oplus m'_{s'-2})$
$s \leftarrow s' - 3$
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 $(m_1, m_2 \ldots m_s)$

Notice that since this construction ensures that there are $\mathsf{AONT.bl}$ bits of "padding" in the second and third to last blocks of the pseudo-message, an $\mathsf{AONT.bl}$ leakage adversary can just choose to not receive the padding, and still be able to compute the inverse function in full, since the padding is always zero. On the other hand, suppose that there existed a $\mathsf{AONT} - \mathsf{IND}$ adversary against AONT, A, then we can construct B, a PRF adversary against block cipher E. ACTUALLY, BOYKO'S PAPER SHOULD HAVE A VALID PROOF.