1 Syntax

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

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

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.

2 Rivest (1997)

$\underline{\mathbf{G}^{\mathrm{ind}}_{\mathsf{AONT}}(A)}$

$b \leftarrow\!\!\$\ \{0,1\}$
$b' \leftarrow\!\!\$\ A^{\mathrm{LR}}$
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**
  $y \leftarrow\!\!\$\ \mathsf{AONT.Transform}(m_1, m_2 \ldots m_s)$
else
  $y \leftarrow\!\!\$\ \mathsf{AONT.Transform}(n_1, n_2 \ldots n_s)$
end
return y

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

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

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

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

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

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

$\quad$ **if** $|M| \neq |N|$ **then**
$\quad\quad$ **return** $\perp$
$\quad$ **end**
$\quad (m_1, m_2 \ldots m_s) \leftarrow M$
$\quad (n_1, n_2 \ldots n_s) \leftarrow N$
$\quad$ **if** $b = 0$ **then**
$\quad\quad y \leftarrow\!\!\$ \mathsf{AONT.Transform}(m_1, m_2 \ldots m_s)$
$\quad$ **else**
$\quad\quad y \leftarrow\!\!\$ \mathsf{AONT.Transform}(n_1, n_2 \ldots n_s)$
$\quad$ **end**
$\quad$ **if** $(|S| \neq |y|) \vee (\mathsf{Hamm}(S) > (|y| - l))$ **then**
$\quad\quad$ **return** $\perp$
$\quad$ **else**
$\quad\quad y \leftarrow y \,\&\, S$
$\quad$ **end**
$\quad$ **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:

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

4 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:

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

5 Relationship between Notions

5.1 $\mathsf{AONT.bl}$-AONT-L $\Longrightarrow$ AONT-IND

Theorem 5.1 *For any AONT-IND adversary A, we can construct $\mathsf{AONT.bl}$-AONT-L adversary B such that*

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

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 To dos

- Prove that the package transform with OAEP/ OWFs work (explicitly) for the Rivest definition/ strong-Rivest definition
- What is AONT used for and what kind of security do we need for that
- What is the application I was thinking of and what kind of security do we need for that?