1 Overview and Literature Review

All-Or-Nothing-Transforms (AONT) refer to keyless, randomized functions that provides leakage resilience for plaintexts, and is proposed as a pre-processing step for many cryptographic applications, such as side-channel attack resistant encryption and secure data-storage. They were introduced by Rivest in [1] in the following terms (rephrased for clarity):

An AONT scheme AONT specifies two algorithms $\mathsf{AONT.Transform}, \mathsf{AONT.Inv}$, as well as integer value $\mathsf{AONT.b}$, referring to the size of the input and output blocks of the scheme. We have that $\mathsf{AONT.Transform} : \{\{0,1\}^{\mathsf{AONT.b}}\}^* \rightarrow \{\{0,1\}^{\mathsf{AONT.b}}\}^*$ and $\mathsf{AONT.Inv} : \{\{0,1\}^{\mathsf{AONT.b}}\}^* \rightarrow \{\{0,1\}^{\mathsf{AONT.b}}\}^*$. We require that for all $x \in$: $\{\{0,1\}^{\mathsf{AONT.b}}\}^*$, $|\mathsf{AONT.Transform}(x)| \geq |x|$. The correctness condition is that $\mathsf{AONT.Inv}(\mathsf{AONT.Transform}(x)) = x$, and the security condition is that "it is computationally infeasible to compute any function of any input message block if any one of the output message blocks is not known."

Here is a run down of the key works in the area that my work will review:

- [1], as above, defined AONT, then proposed an instance of it with the "package transform".
- [2], gives formal game-playing definitions for the security of AONT. Both adaptive and non-adaptive versions of indistinguishability and simulation-based security is discussed. It then makes use of OAEP (in the RO model) to instantiate an AONT scheme that is proven secure.
- [3] defines its own indistinguishability based definition of AONT, and instantiates a provably secure AONT scheme making use of Exposure-Resilient Functions (ERFs). They then show that ERFs can be constructed from any one-way function.
- [4] Chaffing and Winnowing (CW) is a a privacy-preserving scheme that does not make use of encryption in its traditional sense. While CW can be implemented without AONT, the use of AONTs help to decrease the overhead (in bandwidth) introduced by using this scheme.
- [5] Expands on [4], to introduce a security definition for both AONT and CW. It shows that the scheme defined in [4] is not secure under the original security definition of AONTs, but is secure when OAEP is used as the AONT. It provides alternative constructions that are secure under all definitions of AONT thus far.
- [6] applies AONT to make encryption side-channel attack resistent, but does not make use of the security definitions provided, nor present a proof.
- [7] uses AONT to penalize brute force searches by a factor equal to the number of blocks in the ciphertext. This makes use of an asymptotic indistinguishability definition.

2 Proposed Work

My work will be to first review the definitions in [1,2,3] and formalize them. I will then define a unifying definition for AONT that captures the theoretical contributions of [1,2,3], while being usable in security proofs of applications in [4,5,6,7].

3 References

[1] Rivest, R. (1997) *All-Or-Nothing Encryption and The Package Transform*
[2] Boyko, V. (1999) *On the Security Properties of OAEP as an All-or-nothing-Transform*

[3] Canetti, R. et. al (2000) *Exposure-Resilient Functions and All-or-Nothing-Transforms*
[4] Rivest, R. (1998) *Chaffing and Winnowing: Confidentiality without Encryption*
[5] Bellare, M. & Boldyreva A. (2000) *The Security of Chaffing and Winnowing*
[6] McEvoy R. et. al (2014) *All-or-Nothing Transforms as a Countermeasure to Differential Side-Channel Analysis*