A Theory of Weak Combiners

Karthekeyan Chandrasekaran[1] and C. Pandu Rangan(Faculty)[2]

[1] Indian Institute of Technology, Madras ckarthik@cse.iitm.ernet.in
[2] Indian Institute of Technology, Madras rangan@iitm.ernet.in

Abstract. A cryptographic combiner for a primitive P, is a construction that takes as input, candidate primitives and combines them securely to give the primitive P. Such combiners are useful when the security or hardness of the candidate schemes are unknown. The resultant scheme remains secure as long as one of the candidate schemes remains secure.

Several results have been published in this area proving the existence of secure combiners for several primitives and also the impossibility of their existence for certain protocols.

In this work, we give a new definition of combiners by which one can develop combiners using known classes of candidate primitives even with impossibility results under the original definition. The original definition takes all possible candidate primitives into account, while the new definition gives room for special classes of candidate primitives. The new definition basically, weakens the notion of robust combiners to allow for the possibility of existence of combiners that are secure while using certain kinds of candidate primitives and not necessarily secure for all possible candidate primitives. The new definition is thus much closer to reality where we know and work with primitives carrying special properties which could be utilised for securely combining into other primitives.

1 Motivation

According to the definition of robust combiners presented by Naor et. al [1], and used in [2], [3] and [4], an impossibility result regarding the existence of a combiner for a primitive rules out the existence of combiners for all possible candidate primitives. This prevents us from trying to define Combiners which use certain candidate primitives satisfying special properties. In fact, most of the primitives that we know, carry special properties which are omitted while trying to use them as candidates for a combiner. For example, according to [4], the existence of combiners for Collision Resistant Hash(CRH) functions is impossible. However we believe that Combiners could be defined for specific classes of CRH functions. Thus, we need a new definition, under which, the properties satisfied by the primitives could be used advantageously for combining.
Hence, we present a new definition of Combiners which is the relaxed version of robust combiners presented in [1]. Further, we also conjecture the existence of combiners for two candidate hash functions from the Universal Class of Hash functions.

2 Proposed Definitions for Weak Combiners

Definition 1 ((k,m)-weak A-to-B combiner). *Let A and B be crypto- graphic primitives. A (k,m)-weak A-to-B combiner is a PPTM which gets m candidate schemes implementing A as inputs and implements B while satisfying the following two properties:*

1. *If at least k candidates securely implement A, then the combiner securely implements B over most of the parameters of B. To formalise, let S denote the set of all working parameters of B. Then, a weak combiner is efficient for all values in S, except for a polynomial fraction of S.*
2. *The running time of the combiner is polynomial in the security parameter, in m, and in the lengths of the inputs to B.*

We can define Weak Black-Box Combiners, Weak Third-party black-box Combiners and Weak Transparent black-box combiners similarly.

Definition 2 (Weak black-box combiner). *A $(1,2)$-Weak combiner is called a black-box combiner if the following two conditions hold:*

1. *Black-Box Implementation: The combiner is an oracle PPTM given access to the candidates via oracle calls to their implementation function.*
2. *Black-Box Proof: For every candidate there exists an oracle PPTM R^A (with access to A) such that if adversary A breaks the combiner, then R^A breaks the candidate with very high probability.*

Definition 3 (Weak-third-party black-box combiner). *A Weak-third-party black-box combiner is a Weak-black-box combiner where the input candidates behave like trusted third parties. The candidates give no transcript to the players but rather take their inputs and return outputs.*

Definition 4 (Weak transparent black-box combiner). *A Weak-transparent black-box combiner is a Weak-black-box combiner for an interactive primitive where every call to a candidate's next message function is followed by this message being sent to the other party.*

Note : The key difference between a (k,m)-**robust A-to-B combiner** as presented in [2] and our definition of a (k,m)-**weak A-to-B combiner**, is the definition and use of the set S. Our definition expects the combiner to work for all, but a polynomial fraction of values in S. In the earlier definition, the combiner must work for all possible values in S.

To get a clear understanding of the set S in the definition of Weak-Combiners, we apply the same to Collision Resistant Hash functions.

2.1 Weak Combiners for Collision Resistant Hashing(CRH)

We now recast the definition of a robust combiner for CRH [3] to weak combiners for CRH.

Definition 5 *We say that (C, P) is an ϵ-secure collision resistant weak combination if for all $H_1, ..., H_l$ and for polynomial fraction of collisions (M, M') on $C^{H_1,...,H_l}$ we have that*

$$Adv_P[(H_1, ..., H_l), (M, M')] < \epsilon$$

while for the rest of the collisions,

$$Adv_P[(H_1, ..., H_l), (M, M')] > 1 - \epsilon$$

Note : Here, the difference between the definitions is the following, where we define S explicitly. The number of collisions for the hash function $C^{H_1,H_2,...,H_n}$ for which P is not able to output a collision for the candidates $H_1, H_2, ..., H_l$ is a polynomial fraction of the input size for $C^{H_1,H_2,...,H_n}$. That is the number of collisions for which $Adv_P[(H_1, ..., H_l), (M, M')] < \epsilon$ is a polynomial fraction of the number of all possible collisions under $C^{H_1,H_2,...,H_n}$.

Let the set of all collisions under $C^{H_1,H_2,...,H_n}$ be denoted as S. Then,

$$Adv_P[(H_1, ..., H_l), (M, M')] < \epsilon$$

for $|S|/poly(n)$ instances of (M, M') while,

$$Adv_P[(H_1, ..., H_l), (M, M')] > 1 - \epsilon$$

for the remaining instances of (M, M').

3 Significance of the weak definition

As per the strong definition, we will be ruling out the existence of a combiner due to an impossibility result. It is quite possible that the combiner is secure for most inputs of the primitive it is trying to achieve, apart from a polynomial fraction of them. In such cases, the impossibility result under the strong definition completely disables the community from using such combiners. However, if we could characterise such inputs under the definition of weak combiners and avoid using them, then weak-combiners could prove useful in achieving the primitive securely.
Further, to rule out the existence of combiners for a primitive completely, we can try to prove the impossibility results in the weaker definition. Note that the non-existence of combiners under the weaker definition will imply the impossibility of combiners in the usual definition.

We believe the following conjecture is true showing the existence of useful weak combiners for two classes of universal hash functions.

Conjecture 1: Consider the universal classes of hash functions H_1 and H_2 as follows:

- $h : A \to B$, where $A = \{0,1\}^u$, $B = \{0,1\}^b$
  $H_1 = \{h : h(x) = hx$, where h is a random $b \times u$ matrix.$\}$
- $h_{a,b} : A \to B$, where $A = \{0, 1, ..., m-1\}$, $B = \{0, 1, ..., n-1\}$.
  $H_2 = \{h_{a,b} | a, b \in Z_p, a \neq 0\}$, $h_{a,b}(x) = ((ax + b) mod\ p) mod\ n$.

There exists a secure combiner for the two universal classes of hash functions H_1 and H_2.

The above conjecture which we are in the process of proving, essentially validates the existence of Combiners for CRH functions under the weak definition but not under the stronger definition, as being used currently. Thus, our new definition seems much more practical and useful for cryptographic applications.

References

[1] D. Harnik, J. Kilian, M. Naor, O. Reingold and A. Rosen. On Robust Combiners for Oblivious Transfer and Other primitives. In *Proc. Eurocrypt '05*, pages 96-113, 2005.

[2] R.Meier and B.Przydatek. On Robust Combiners for Private Information Retrieval and Other Primitives. In *Advances in Cryptology - Crypto 2006*, volume 4117 in LNCS, pages 555-569. Springer-Verlag, 2006.

[3] D. Boneh and X. Boyen. On the Impossibility of Efficiently Combining Collision Resistant Hash Functions. In *Advances in Cryptology - Crypto 2006*, volume 4117 in LNCS, Springer-Verlag, 2006.

[4] K Pietrzak. Non-Trivial Black-Box Combiners for Collision-Resistant Hash-Functions don't Exist. In *Cryptology ePrint Archive*, Report 2006/348, 2006. http://eprint.iacr.org/.