On the Impossibilities of Basing One-Way Permutations on Central Cryptographic Primitives

Yan-Cheng Chang
Department of Computer Science and Information Engineering
National Taiwan University
Taipei, Taiwan
Email: r88023@csie.ntu.edu.tw

Chun-Yun Hsiao
Computer Science Department
Boston University
U.S.A.
Email: cyhsiao@cs.bu.edu

Chi-Jen Lu
Institute of Information Science
Academia Sinica
Taipei, Taiwan
Email: cjlu@iis.sinica.edu.tw

Abstract

We know that trapdoor permutations can be used to construct all kinds of basic cryptographic primitives, including trapdoor functions, public-key encryption, private information retrieval, oblivious transfer, key agreement, and those known to be equivalent to one-way functions such as digital signature, private-key encryption, bit commitment, pseudo-random generator and pseudo-random functions. On the other hand, trapdoor functions are not as powerful as trapdoor permutations, so the structural property of permutations seems to be something special that deserves a more careful study. In this paper, we investigate the relationships between one-way permutations and all these basic cryptographic primitives. Following previous works, we focus on an important type of reductions called black-box reductions. We prove that no such reductions exist from one-way permutations to either trapdoor functions or private information retrieval. Together with previous results, all the relationships with one-way permutations have now been established, and we know that no such reductions exist from one-way permutations to any of these primitives except trapdoor permutations. This may have the following meaning, with respect to black-box reductions. We know that one-way permutations imply none of the primitives in "public cryptography", where additional properties are required on top of "one-wayness" [12], so permutations cannot be traded for any of these additional properties. On the other hand, we now know that none of these additional properties can be traded for permutations either. Thus, permutation seems to be something orthogonal to those additional properties on top of one-wayness. Like previous non-reducibility results [12, 21, 23, 17, 7, 9, 8, 6], our proofs follow the oracle separation paradigm of Impagliazzo and Rudich [12].

Keyword: Cryptographic Primitives, Black-Box Reductions, One-Way Permutations, Trapdoor Functions, Private Information Retrievals.

1 Introduction

Modern cryptography has provided us with all kinds of protocols for various interesting and important tasks involving security issues. However, almost all of these protocols have their securities based on some intractability assumptions which all imply $\mathcal{P} \neq \mathcal{NP}$. So unconditional proofs of security for these protocols may seem far beyond our reach. One important line of research then is to understand the relationships among these assumptions. However, there are many interesting cryptographic tasks, and even a single task may be several variants. So potentially the whole picture could become very messy and have little help in clarifying our understanding. Instead, we want to focus on the most basic cryptographic tasks in their most primitive forms, which can serve as building blocks for more advanced protocols. We will also restrict ourselves to the classical world of cryptography, and leave the questions in quantum cryptography for future studies.

According to [7], such basic cryptographic primitives can be roughly divided into two categories: private cryptography and public cryptography.[1] Private cryptography is represented by private-key encryption, and includes one-way permutation (OWP), one-way function (OWF), pseudo-random generator (PRG), pseudo-random function (PRF), bit commitment (BC), and digital signature (DS). Public cryptography is represented by public-key encryption (PKE), and includes trapdoor permutation (TDP), trapdoor function (TDF), oblivious transfer (OT), private information retrieval (PIR), and key agreement (KA). "One-wayness" turns out to be essential as these primitives all are known to imply one-way functions [11, 19, 1, 2, 7]. For private cryptography, one-wayness basically is also sufficient as one-way functions can be used to construct all the primitives therein, except one-way permutations. For public cryptography, additional properties are required on top of one-wayness, and the relationships among primitives appear to be rather complicated. We know that trapdoor permutations imply all of them, but some implications among others are known to fail, in the sense to be discussed next.

It is not clear what it means that one primitive Q does not imply the other primitive P, or equivalently P can not be reduced to Q, especially when both primitives exist under some plausible assumptions. After all, if the primitive P exists, there is a protocol of P based on Q that simply ignores Q. Impagliazzo and Rudich [12] introduced a restricted but important subclass of reductions called *black-box reductions*. Informally speaking, a black-box reduction from P to Q is a construction of P out of Q that ignores the internal structure of the implementation of Q. Furthermore, the security of P's implementation can also be guaranteed in a black-box way that one can use any adversary breaking P as a subroutine to break Q. In fact in cryptography, almost all constructions of one primitive from another known so far are done in this way, so it makes sense to focus on reductions of this kind. Hereafter, all the reductions or implications we refer to in this paper will be black-box ones. To prove that no black-box reduction exists from P to Q, it suffices to construct an oracle relative to which Q exists whereas P does not. Using this approach, Impagliazzo and Rudich [12] showed that no such black-box reduction exists from KA to OWP. As every primitive in public cryptography implies KA [1, 4, 7], this provides a strong evidence that primitives in public cryptography requires strictly more than one-wayness. Since then, more and more separations between cryptographic primitives have been established following this paradigm [21, 23, 17, 7, 9, 8, 6].

[1] We want to remark that this classification is just a convenient one for us and is by no means a precise or complete one. The situation becomes complicated when one wants to talk about variations of primitives meeting additional requirements (e.g. [23, 6]).

We know that trapdoor permutations imply all those basic cryptographic primitives, but it is not the case for trapdoor functions as they do not imply OT [7] and thus PIR [4]. So there seems to be something special for being a permutation which deserves further study. We also know that one-way functions do not imply one-way permutations [20, 16], so permutation does not seem to be a property that one can have for free. We know that one-way permutations imply none of the primitives in public cryptography [12], so on top of one-wayness, one can not trade permutations for any of the additional properties required in public cryptography. Then, the question we want to ask is: can any of those additional properties required in public cryptography be traded for permutations? Formally, can any of the primitives except TDP in public cryptography imply OWP? Figure 1 summarizes the relationships known so far between primitives and OWP. We will show that neither TDF nor PIR implies OWP, so the answer to that question is actually no!

$$\begin{tikzcd}
& \mathrm{TDF} \arrow[r] & \mathrm{PKE} \arrow[dr] & & \mathrm{OWP} \arrow[dl, "/" marking] \arrow[dd, shift right] \\
\mathrm{TDP} \arrow[ur] \arrow[dr] & & & \mathrm{KA} \arrow[dr] & \\
& \mathrm{PIR} \arrow[r] & \mathrm{OT} \arrow[ur] & & \mathrm{OWF, PRG, PRF, BC, DS} \arrow[uu, shift right, "/" marking]
\end{tikzcd}$$

Figure 1: Relationships between OWP and other cryptographic primitives

We first construct an oracle, relative to which a collection of (injective) trapdoor functions (TDF) exists whereas OWP does not. As TDF implies PKE [24] and PKE (two-pass KA) implies KA, we establish the impossibility of having black-box reductions from OWP to either TDF, PKE, or KA. Next, we construct an oracle, relative to which PIR exists whereas OWP does not. Because PIR implies OT [4], we establish that no black-box reduction exists from OWP to either PIR or OT. One immediate corollary is that PIR does not imply TDP, in contrast to the known result that TDP does imply PIR [15]. So according to our results, none of the primitives in public cryptography implies OWP in a black-box way. This is interesting in the sense that all the powerful primitives, except TDP, in public cryptography, which make almost all of conceivable cryptographic tasks possible, are still unable to yield OWP. Our results suggest that permutation is really a special property that is orthogonal to other additional properties required in cryptography. Furthermore, the reducibility from each primitive to OWP was already known before, so now all the relationships, with respect to black-box reductions, between one-way permutations and those basic cryptographic primitives have been established. However, we want to stress that we are still far from being able to settle the real relationships among primitives, and in fact, to have separations beyond black-box reductions would require some major breakthrough in complexity theory [12].

For each separation between primitives, we need to find a suitable oracle that is powerful enough for making one primitive possible, but still not so for the other. We basically follow the approach of Impagliazzo and Rudich [12] and Gertner *et al.* [7]. It is known that a random function is one-way with high probability, even relative to a $\mathcal{PSPACE}$-complete function [12]. Then, OWF exists relative to an oracle containing a random function and a $\mathcal{PSPACE}$-complete function, but on the other hand, OWP does not relative to such an oracle [20, 16]. We want to separate OWP from TDF and PIR. Each time we look for a special function which realizes the additional property required by that primitive but does not yield permutations. By adding such a function to the oracle, we can build the corresponding primitive, TDF or PIR, but relative to the oracle, OWP still does not exist. Our strategy of finding such special functions is based on the observation that both TDF and PIR can be seen as two-party primitives while OWP involves only one party. So we look for those functions that are useful in a two-party setting but useless in a one-party case.

The rest of the paper is organized as follows. In Section 2, we describe our notation and provide definitions for the cryptographic primitive involved in this paper. Then in Section 3 and 4, we prove that no black-box reductions exist from OWP to TDF and PIR, respectively.

2 Notation and Definitions

Let $[n]$ denote the set $\{0, 1, \ldots, n-1\}$. For $x \in \{0,1\}^n$, let $x[i]$ denote the i-th bit of x if $i \in [n]$, and an arbitrary value, say 0, otherwise. We write $poly(n)$ to denote a polynomial in n. We write $*$ for $\{0,1\}^*$ and $(*, q, *)$ for those (u, q, v) with $u, v \in \{0,1\}^*$. For a distribution S, we write $s \in S$ to denote sampling s according to the distribution S. For any $n \in \mathbb{N}$, let U_n denote the uniform distribution over $\{0,1\}^n$.

Parties in cryptographic primitives are assumed to run in polynomial time, and are modeled by probabilistic polynomial-time Turing machines (PPTM). Each cryptographic primitive is associated with a security parameter k, for evaluating how secure that primitive is. A function is called negligible if it vanishes faster than any inverse polynomial. We say that two distributions X and Y over $\{0,1\}^k$ cannot be distinguished if for any PPTM M,

$$\left| \Pr_{x \in X}[M(x) = 1] - \Pr_{y \in Y}[M(y) = 1] \right| \leq \delta(k),$$

for some negligible function $\delta(k)$. We say a function is easy to compute if it is computable in polynomial time. We say that a function f is hard to invert if for any PPTM M,

$$\Pr_{x \in U_k}[f(M(f(x))) = f(x)] \leq \delta(k),$$

for some negligible function $\delta(k)$.

In the following, we give brief definitions of the cryptographic primitives studied in this paper. More formal treatment can be found in standard textbooks or the original papers. The most fundamental primitive is *one-way function*, which is essential to all cryptographic primitives.

Definition 1. *A one-way function (OWF) is a function that is easy to compute but hard to invert.*

From one-way functions, we define primitives with additional properties. A one-way permutation is a one-way function that is itself a permutation.

Definition 2. *A one-way permutation (OWP) is a one-way function f with the additional requirement that for every $k \in \mathbb{N}$, f maps $\{0,1\}^k$ to $\{0,1\}^k$ in a one-to-one and onto way.*

Trapdoor functions are one-way functions which, when given some additional *trapdoor* information, are easy to invert.

Definition 3. *A collection of trapdoor functions (TDF) is a collection of function families $\mathcal{F} = \{\mathcal{F}_k | k \in \mathbb{N}\}$ satisfying the following properties.*

- *There is a PPTM I, that on input 1^k outputs a pair (f, t), where f is (an index of) a function in $\mathcal{F}_k$ and t is a string called the* trapdoor *for f.*

References

[1] Mihir Bellare, Shai Halevi, Amit Sahai, and Salil P. Vadhan. Many-to-one trapdoor functions and their relation to public-key cryptosystems. In Hugo Krawczyk, editor, *Advances in Cryptology—CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 283-298. Springer-Verlag, 1998.

[2] Amos Beimel, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. One-way functions are essential for single-server private information retrieval. In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing*, pages 89-98, 1999.

[3] Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private information retrieval. In *Proceedings of the 36th Annual ACM Symposium on Theory of Computing*, pages 41-50, 1995.

[4] Giovanni Di Crescenzo, Tal Malkin, and Rafail Ostrovsky. Single database private information retrieval implies oblivious transfer. In Bart Preneel, editor, *Advances in Cryptology—EUROCRYPT '00*, volume 1807 of *Lecture Notes in Computer Science*, pages 122-138. Springer-Verlag, 2000.

[5] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644-654, 1976.

[6] Marc Fischlin. On the impossibility of constructing non-interactive statistically-secret protocols from any trapdoor one-way function. In Bart Preneel, editor, *Topics in Cryptology—CT-RSA '02*, volume 2271 of *Lecture Notes in Computer Science*, pages 79-95. Springer-Verlag, 2002.

[7] Yael Gertner, Sampath Kannan, Tal Malkin, Omer Reingold, and Mahesh Viswanathan. The relationship between public key encryption and oblivious transfer. In *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science*, pages 325-335, 2000.

[8] Yael Gertner, Tal Malkin, and Omer Reingold. On the impossibility of basing trapdoor functions on trapdoor predicates. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science*, pages 126-135, 2001.

[9] Rosario Gennaro and Luca Trevisan. Lower bounds on the efficiency of generic cryptographic constructions. In *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science*, pages 305-313, 2000.

[10] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364-1396, 1999.

[11] Russell Impagliazzo and Michael Luby. One-way functions are essential for complexity based cryptography (extended abstract). In *Proceedings of the 30th Annual IEEE Symposium on Foundations of Computer Science*, pages 230-235, 1989.

[12] Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, pages 44-61, 1989.

[13] Joe Kilian. Founding cryptography on oblivious transfer. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, pages 20-31, 1988.

[14] Eyal Kushilevitz and Rafail Ostrovsky. Replication is not needed: single database, computationally-private information retrieval. In *Proceedings of the 38th Annual IEEE Symposium on Foundations of Computer Science*, pages 364-373, 1997.

[15] Eyal Kushilevitz and Rafail Ostrovsky. One-way trapdoor permutations are sufficient for non-trivial single-server private information retrieval. In Bart Preneel, editor, *Advances in Cryptology—EUROCRYPT '00*, volume 1807 of *Lecture Notes in Computer Science*, pages 104-121. Springer-Verlag, 2000.

[16] Jeff Kahn, Michael E. Saks, and Cliff Smyth. A dual version of Reimer's inequality and a proof of Rudich's conjecture. In *Proceedings of the 15th Annual IEEE Conference on Computational Complexity*, pages 98-103, 2000.

[17] Jeong Han Kim, Daniel R. Simon, and Prasad Tetali. Limits on the efficiency of one-way permutation-based hash functions. In *Proceedings of the 40th Annual IEEE Symposium on Foundations of Computer Science*, pages 535-542, 1999.

[18] Moni Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, 4(2):151-158, 1991.

[19] John Rompel. One-way functions are necessary and sufficient for secure signatures. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, pages 387-394, 1990.

[20] Steven Rudich. Limits on the provable consequences of one-way functions. *Ph.D. thesis*, U.C. Berkeley, 1988.

[21] Steven Rudich. The use of interaction in public cryptosystems (extended abstract). In Joan Feigenbaum, editor, *Advances in Cryptology—CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 242-251. Springer-Verlag, 1991.

[22] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120-126, 1978.

[23] Daniel R. Simon. Finding collisions on a one-way street: can secure hash functions be based on general assumptions? In Kaisa Nyberg, editor, *Advances in Cryptology—EUROCRYPT '98*, volume 1403 of *Lecture Notes in Computer Science*, pages 334-345. Springer-Verlag, 1998.

[24] Andrew Chi-Chih Yao. Theory and applications of trapdoor functions (extended abstract). In *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science*, pages 80-91, 1982.