A Simple and Unified Method of Proving Indistinguishability
(Extended Abstract)

Mridul Nandi

David R. Cheriton School of Computer Science, University of Waterloo, Canada
m2nandi@cs.uwaterloo.ca

Abstract. Recently Bernstein [4] has provided a simpler proof of indistinguishability of CBC construction [3] which is giving insight of the construction. Indistinguishability of any function intuitively means that the function behaves very closely to a uniform random function. In this paper we make a unifying and simple approach to prove indistinguishability of many existing constructions. We first revisit Bernstein's proof. Using this idea we can show a simpler proof of indistinguishability of a class of DAG based construction [8], XCBC [5], TMAC [9], OMAC [7] and PMAC [6]. We also provide a simpler proof for stronger bound of CBC [1] and a simpler proof of security of on-line Hash-CBC [2]. We note that there is a flaw in the security proof of Hash-CBC given in [2]. This paper will help to understand security analysis of indistinguishability of many constructions in a simpler way.

1 Introduction

This paper deals how one can obtain a simple proof for a bound of distinguishing advantage of two classes of object, mainly two classes of functions. We consider several constructions and show how simply the distinguishing advantage can be obtained. Here we mainly consider distinguishing attack of existing constructions with popularly known *random function* (in this paper, we term it as ***uniform random function*** [4]). *Indistinguishability* of a construction intuitively means that there is no efficient distinguisher which distinguishes this from the uniform random function. Bernstein has provided a simple proof of indistinguishability of **CBC-MAC** (*Cipher Block Chaining-Message Authentication Code*) [4] which is the main motivation of this paper. We first revisit his proof [4] and show how simply one can extend the proof idea for a class of **DAG** (*Directed Acyclic Graph*) based general construction due to Jutla [8]. This class contains many constructions including CBC and a variant of PMAC [6]. We give a simpler proof of partial result of improved security analysis of CBC-MAC [1]. We also study distinguishing advantage with a different class known as *uniform random on-line function* introduced in Crypto 2001 [2]. We show that same idea of proof is also applicable in this scenario and we obtain a simpler proof of Hash-CBC construction [2]. The idea of all these proofs is based on statistical distribution of the *view of the distinguisher*.

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 317–334, 2006.

Thus, it gives information theoretic security and hence the security bound holds for computationally unbounded distinguishers also.

This simple idea can help to understand better about the insight of the construction and can help to come up with very nice constructions and results. For example, we modify slightly the DAG based class due to Jutla [8], so that it will include all known constructions like XCBC [5], TMAC [9], OMAC [7], PMAC [6] etc.

Organization of the paper. In this paper, we first build mathematics for the security bound of the distinguisher in Section 2 which would be used throughout the paper. Then we rewrite the simple proof of security of CBC given by D. J. Bernstein in Section 3 and we show a similar result in case of CBC based on uniform random permutation. In Section 4, we generalize his idea of proof to have a simple proof for a general class proposed by Jutla. We see that security of arbitrary length MAC construction like XCBC, TMAC, OMAC, PMAC etc. can be derived from it. In Section 5 we provide a simpler proof of security of Hash-CBC. We note that in the original paper there is a flaw in the proof. Finally we conclude.

2 Mathematics for Security Proof in Distinguishing Attack

2.1 Different Notion of Distances and Its Cryptographic Significance

(1) Statistical Distance: Let X and Y be two random variables taking values on a finite set S. We define *statistical distance* between two random variables by

$$\mathrm{d}_{\mathrm{stat}}(X,Y) := \max_{T\subset S} \left|\Pr[X\in T] - \Pr[Y\in T]\right|.$$

Note that, $\Pr[X \in T] - \Pr[Y \in T] = \Pr[Y \notin T] - \Pr[X \notin T]$ and hence $\mathrm{d}_{\mathrm{stat}}(X,Y) = \max_{T\subset S}\Pr[X \in T] - \Pr[Y \in T]$. It measures the distance between the distribution of the random variables. In fact, it is really a *metric* or *distance function* on the set of all distributions on S. It measures how close their distributions are. For identically distributed random variables X and Y, $\mathrm{d}_{\mathrm{stat}}(X,Y) = 0$ and if the random variables are disjoint[1] then the statistical distance is one. In all other cases it lies between zero and one. Now we prove an equivalent definition of statistical distance and study some standard examples. Proof of all lemmas stated in this section are given in Appendix A.

Lemma 1. $\mathrm{d}_{\mathrm{stat}}(X,Y) = \Pr[X \in T_0] - \Pr[Y \in T_0] = \frac{1}{2} \times \sum_{a\in S} \left|\Pr[X = a] - \Pr[Y = a]\right|$, *where* $T_0 = \{a \in S : \Pr[X = a] \geq \Pr[Y = a]\}$.

[1] X and Y are said to be disjoint if X occurs with some positive probability then Y does occur with probability zero and vice versa. More precisely, there exists a subset T such that $\Pr[X \in T] = 1$ and $\Pr[Y \in T] = 0$.