# HCH: A New Tweakable Enciphering Scheme Using the Hash-Encrypt-Hash Approach

Debrup Chakraborty[1] and Palash Sarkar[2]

[1] Computer Science Department
CINVESTAV-IPN
Mexico, D.F., 07360, Mexico
debrup@cs.cinvestav.mx
[2] Applied Statistics Unit
Indian Statistical Institute
Kolkata 700108, India
palash@isical.ac.in

**Abstract.** The notion and the first construction of a tweakable enciphering scheme, called CMC, was presented by Halevi-Rogaway at Crypto 2003. In this paper, we present HCH, which is a new construction of such a scheme. The construction uses the hash-encrypt-hash approach introduced by Naor-Reingold. This approach has recently been used in the constructions of tweakable enciphering schemes HCTR and PEP. HCH has several advantages over the previous schemes CMC, EME, EME*, HCTR, and PEP. CMC, EME, and EME* use two block-cipher invocations per message block, while HCTR, PEP, and HCH use only one. PEP uses four multiplications per block, while HCTR and HCH use only two. In HCTR, the security bound is cubic, while in HCH security bound is quadratic.[1]

**Keywords:** modes of operations, tweakable encryption, strong pseudo-random permutation.

## 1 Introduction

A block cipher is one of the basic primitives used in cryptography. Depending upon the application goals, there are many uses of a block cipher. A particular method of using a block cipher is called a mode of operation. The literature describes different modes of operations of a block cipher achieving goals such as confidentiality, authentication, authenticated encryption, etcetera. For several years, NIST of USA [1] has been running an open domain process to standardize modes of operations for achieving various functionalities. Currently, there are around twenty different modes of operations proposals for different tasks.

One particular interesting functionality is a tweakable enciphering scheme [4]. (We note that this functionality is currently not covered by NIST's standardization efforts.) This is based on the notion of tweakable block ciphers introduced

[1] The last three sentences of the abstract are due to a reviewer who suggested that these accurately capture the contribution of the paper.

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 287–302, 2006.

in [6]. A tweakable enciphering scheme is a length preserving encryption protocol which can encrypt messages of varying lengths. The security goal is to satisfy the notion of the tweakable strong pseudo-random permutation (SPRP). As pointed out in [4], one of the most important applications of a tweakable enciphering scheme is disk encryption. Currently, there are several proposals CMC [4], EME [5], EME* [3], HCTR [9] and PEP [2] for tweakable enciphering schemes.

*Our Contribution:* In this paper, we present HCH, which is a construction of a new tweakable enciphering scheme. HCH uses a single key, can encrypt arbitrary length messages and has a quadratic security bound. Our construction is based on HCTR. It uses a counter mode of encryption sandwiched between two polynomial hashes. HCTR uses two keys and has a cubic security bound. To avoid these problems, we use certain ideas (and analysis) from PEP. In particular, the idea of appropriately encrypting the tweak and the message length is adopted from PEP. In addition, we initialize the counter mode by the output of a block cipher encryption; a feature not present in HCTR. The combination of all these features leads us to the desired goal.

HCH is based on the hash-encrypt-hash approach to the construction of strong pseudo-random permutation. The hash is a Wegman-Carter [10] type of polynomial hash. This approach was originally suggested by Naor-Reingold [8,7], though they did not consider tweaks, a notion which appeared later in the literature. The constructions HCTR and PEP are also based on the hash-encrypt-hash approach. On the other hand, CMC [4] introduced the encrypt-mask-encrypt approach, i.e., to have two layers of encryption with a masking layer in-between. CMC used CBC for the encryption layer, while the later works EME and EME* used ECB for the encryption layers.

In terms of efficiency, HCH and HCTR have roughly the same efficiency; HCH performs a few extra block cipher invocations, while HCTR performs a few extra $GF(2^n)$ multiplications. In a sequential mode, HCH is faster than PEP; though in a parallel mode all three of HCTR, PEP and HCH have roughly the same efficiency. The comparison to CMC (and EME*) depends on the relative efficiency of a block cipher invocation and a $GF(2^n)$ multiplication. It is currently believed, that a single AES-128 invocation is faster than a $GF(2^n)$ multiplication. Hence, used with AES-128, CMC will be faster than HCH (or HCTR, PEP). On the other hand, if one invocation of the underlying block cipher is slower than one $GF(2^n)$ multiplication, then HCH (and HCTR, PEP) will be faster than CMC. Thus, the comparison is really between the two approaches rather than individual constructions. We believe both approaches are interesting and can be pursued further.

## 2 Specification of HCH

We construct the tweakable enciphering scheme HCH from a block cipher $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ and call it HCH[$E$]. The key space of HCH[$E$] is same as that of the underlying block cipher $E$ and the tweak space is $\mathcal{T} = \{0,1\}^n$. The message space consists of all binary strings of length greater than $n$.