Enciphering with Arbitrary Small Finite Domains

Valery Pryamikov

Harper Security Consulting, Vestre Rosten 81, 7075 Trondheim, Norway
valery@harper.no

Abstract. In this paper we present a new block cipher over a small finite domain $\mathcal{T}$ where $|\mathcal{T}| = k$ is either 2^{16} or 2^{32} . After that we suggest a use of this cipher for enciphering members of arbitrary small finite domains $\mathcal{M}$ where $\mathcal{M} \subseteq \mathcal{T}$. With cost of an extra mapping, this method could be further extended for enciphering in arbitrary domain $\mathcal{M}'$ where $|\mathcal{M}'| = k' \leq k$. At last, in a discussion section we suggest a few interesting usage scenarios for such a cipher as an argument that enciphering with arbitrary small finite domains is a very useful primitive on its own rights, as well as for designing of a higher level protocols.

Keywords: Block Ciphers, Symmetric Encryption, Pseudorandom Permutations, Modes of Operations.

1 Introduction

Our motivation for this research was ignited by an obvious dissonance. Pseudo-random permutations are a very useful tool for many tasks, starting from the shuffling of a card deck to generation of bankcard numbers, pin codes and one time passwords, collecting samples from real-time data and many more. There is a tool that conveniently defines families of pseudo-random permutations - block ciphers. The modern block ciphers have very strong pseudo-random properties, compactly index selected permutation by an encryption key, and operate with block size that is very well suited for secure encryption of large amount of data. However, the large domains of the modern block ciphers make the size of their pseudo-random permutation too big for being practical for the tasks outlined above. The task of enciphering in arbitrary finite domain was previously considered by creators of Hasty Pudding Cipher, Schroeppel and Orman [13][1]. Later a rigorous treatment of the iterative encryption method, together with two other methods of encryption messages in arbitrary finite domains, were presented in a paper of Black and Rogaway [1]. Another method of construction of variable input length ciphers was also presented earlier in [2].

However, in cases when the size of required permutation is small, the previously suggested techniques either don't work [2] or become quite inefficient [13, 1], especially when considering small 8-bits microcontrollers.

[1] Schroeppel believes that the idea of iterative application of the encryption until proper domain point is reached, dates back to the rotor machines used in the early twentieth century.

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 251–265, 2006.

To solve this task we have designed a cipher with a small block size of either 16 or 32 bits that we named TinyPRP. The TinyPRP cipher is key-alternating block cipher [5] that uses wide trail design strategy [3, 5] – the methodology of AES [4, 5] cipher. Additionally, TinyPRP cipher reuses some of the elements of the AES cipher, such as AES's S-box with optimal linear and differential resistance properties. In order to fit the small block size, we have designed the linear step of the round transformation function of our cipher in a different way than AES, however it is also based on Maximum Distance Separable codes and provide the maximal branch number that we could have achieved with such a small block size. Analogously to AES, TinyPRP cipher could be efficiently implemented in software and hardware, including but not limited to small 8-bits microcontrollers.

Due to a small block size, the security goals of the design of TinyPRP cipher follows definitions from [1] and could be outlined as: even when an adversary having access to the encryption oracle, has collected encryption of all but the two last points of the domain, the adversary should not be able to distinguish encryptions of the remaining two points significantly better than a random guess.

TinyPRP is very well suited for the tasks such as non-expanding encryption of small fields of database, for example numeric fields, that are usually smaller than the block size of standard symmetric encryption algorithms such as AES. Note, that we are not encouraging the use of TinyPRP for encryption of large messages – where the standard ciphers such as AES is a superior choice.

When used together with iterative encryption until the proper domain point is reached of [13, 1], TinyPRP cipher provides efficient method of encrypting messages in arbitrary small domain, that could be used for tasks such as shuffling a card deck, generation and verification of pin codes and onetime passwords, generation and verification of onetime credit card numbers, and many others.

In this paper we present design of the TinyPRP cipher. Reference implementation of the key elements of the algorithm is presented in appendixes. A complete reference implementation of the cipher could be downloaded from the authors website [14].

2 TinyPRP Specification

TinyPRP is an iterated block cipher with a variable block length and a variable key length. The cipher supports the block length of 16 or 32 bits and the key length of 96 or 128 bits that could be independently specified[2] . The cipher iteratively transforms the intermediate state that has the size of block. The state is initialized with a block of plain text before application of the algorithm. The cipher starts and ends with addition of round key[3] which we denote as function

[2] The algorithm allows selecting key size as any multiple of 32 bits, however the key sizes below 96 bits are considered as insecure and should be used for experimenting purposes only.

[3] Any transformation of the state before the first addition of the round key or after the last addition of the round key is known and therefore could be easily factored out by cryptanalyst.