International Journal of Innovative Computing, Information and Control
Volume **7**, Number **8**, August **2011**

ICIC International ©2011 ISSN 1349-4198
pp. **4941–4954**

FAST MULTI-CIPHER TRANSFORMATION AND ITS IMPLEMENTATION FOR MODERN SECURE PROTOCOLS

Chung-Ping Young[1], Chung-Chu Chia[1], Yen-Bor Lin[1] and Liang-Bi Chen[2]

[1]Department of Computer Science and Information Engineering
National Cheng Kung University
No. 1, University Road, Tainan City 701, Taiwan
p7894120@mail.ncku.edu.tw

[2]Department of Computer Science and Engineering
National Sun Yat-Sen University
No. 70, Lien-Hai Road, Kaohsiung 80424, Taiwan
liangbi@eslab.cse.nsysu.edu.tw

Received March 2010; revised July 2010

Abstract. *This paper proposes a fast multi-cipher transformation (FMCT) scheme which enables a cryptosystem to employ multiple cipher algorithms concurrently and efficiently in a session of communication. A file can be encrypted by different cipher algorithms with diverse parameters through FMCT. We prove that a cryptosystem based on FMCT is reversible, flexible, workable and applicable in modern secure protocols. For high throughput applications based on FMCT cryptosystem, a multi-core scheduling algorithm is also proposed. Since this scheduling algorithm spans a lot of FPGA configuration files from base cipher algorithms, even if the number of base cipher algorithms is limited, a lot of configurations of cipher suits can be generated for cipher change protocol in different session of communications. Therefore, the frequency of the usage of a certain cipher algorithm is effectively reduced. No doubt, this is an alternative way to promote higher security in modern secure protocols.*
Keywords: Multi-cipher, Multi-mode, Hardware scheduling, Secure protocols

1. **Introduction.** Multi-cipher [1] and multi-mode [2] schemes are employed to strengthen the secret-key ciphers in SSL and IPsec. A multi-cipher cryptosystem is able to delete broken algorithms or add new algorithms, and it can use a different secret-key cipher in a different session of communication. Since the cipher algorithms are not used simultaneously, the FPGA devices are recommended [3] to implement the supporting hardware accelerators for reconfigurability and resource efficiency [4]. Multi-mode operation refers to a cryptosystem in which secret-key ciphers are employed with different operation modes, such as electronic codebook (ECB), cipher block chaining (CBC), cipher feedback (CFB), output feedback (OFB) and counter (CTR). Except for the ECB mode, each mode needs an initialization vector (IV).

Although current secure protocols are flexible to change cipher algorithms and operation modes, most of the supporting hardware accelerators only perform one cipher algorithm and one operation mode in a session of communication. If we can download all the different hardware accelerators for different sessions of communications into a reconfigurable device at a time, the switching overhead of cipher change operation can be reduced. Since each hardware accelerator is designed for a specific cipher algorithm with its operation mode, when a group of accelerators coexist, it requires a suitable scheduling algorithm to make them cooperate efficiently. There has been hardly any work which can process multiple cipher algorithms at one time with diverse parameters, such as operation