

## Design and Implementation of CSP Module

Rao Wenbi<sup>1</sup>, Xiong Huiyue<sup>2</sup>, Tang Chunming<sup>3</sup>, Li Wei<sup>4</sup>

<sup>12</sup>School of Computer Science and Technology, Wuhan University of Technology  
Wuhan, Hubei, 430070, China

Email: raowenbi@yahoo.com.cn Tel: +86(0) 2752236288

<sup>3</sup>Information and Communication Engineering College, Harbin Engineering University

<sup>4</sup>Department of Computer and Systems Sciences, Royal Institute of Technology  
Stockholm, 16440, Sweden

Email: liwei@dsv.su.se Tel: +46(0)8161662

### ABSTRACT

Along with fast development of Internet, the communicating degree of information is more improved. Cryptographic technology is used in the course of information communicate, since the problem of information security is outstanding increasingly. CSP, which is used to implement cryptographic operations, is the base of Microsoft's security applications frame and serves, but it can only be used in Windows Operating System and the speed of cryptographic operations is limited due to its software implementation. In order to resolve the above problems and really meet Chinese cryptographic standards, a new CSP module named as XyCSP which make the CSPs of Microsoft as reference, is designed in this paper. The design and implementation of XyCSP with three forms and the procedure of writing XyCSP module are all presented. Therefore the application developer can encrypt and decrypt the message with CryptoAPI and keep the message securely transmission.

**Keywords:** XyCSP, design, CryptoAPI, Cryptographic technology