ISO/IEC TR 24485:2022-10 (E)

Information security, cybersecurity and privacy protection - Security techniques - Security properties and best practices for test and evaluation of white box cryptography

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Security properties of white box cryptography 2
4.1 Implementation of a white box cryptography 2
4.1.1 General 2
4.1.2 Description of a WBC 2
4.1.3 Adherence between WBC code and the device hosting it 3
4.2 WBC attack path(s) 3
4.2.1 General 3
4.2.2 De-embedding of code (code lifting) 3
4.2.3 Device analysis 4
4.2.4 Code analysis 4
4.3 WBC usages 4
4.3.1 General 4
4.3.2 Symmetric encryption 5
4.3.3 Asymmetric encryption / signature 5
4.3.4 Keyed hash function 5
4.3.5 Customized cryptographic algorithm 5
4.4 Security properties 5
4.4.1 General 5
4.4.2 Secrecy of the key 5
4.4.3 Difficulty to attack diversified instance 6
4.4.4 Difficulty to lift the code 6
4.4.5 Difficulty to reverse-engineer the binary / obfuscation code 6

5 Best practices for WBC 7
5.1 Tests condition 7
5.1.1 General 7
5.1.2 WBC under source code version 7
5.1.3 WBC under compiled code version 7
5.1.4 Best practices for testing 7
5.2 Security tests 7
5.2.1 General 7
5.2.2 Testing the key secrecy 7
5.2.3 Testing the difficulty to attack diversified instances 7
5.2.4 Testing the difficulty to lift the code 8
5.2.5 Testing the difficulty to reverse-engineer the binary / obfuscation code 8

6 Best practices for WBC 8
6.1 General 8
6.2 Core analyses 8

6.2.1 General 8
6.2.2 Cryptanalytic analysis of tables 8
6.2.3 Side-channel analysis on WBC 8
6.2.4 Fault injection analysis on WBC 9
6.2.5 Evaluation involving combined techniques 9
6.3 Analysis aiming at circumventing access to the plain WBC protection 9
6.3.1 General 9
6.3.2 Reverse-engineering of the binary code 9
6.3.3 Space hardness evaluation 9

Annex A (informative) Design of white-boxing-friendly cryptographic algorithms 10

Bibliography 11