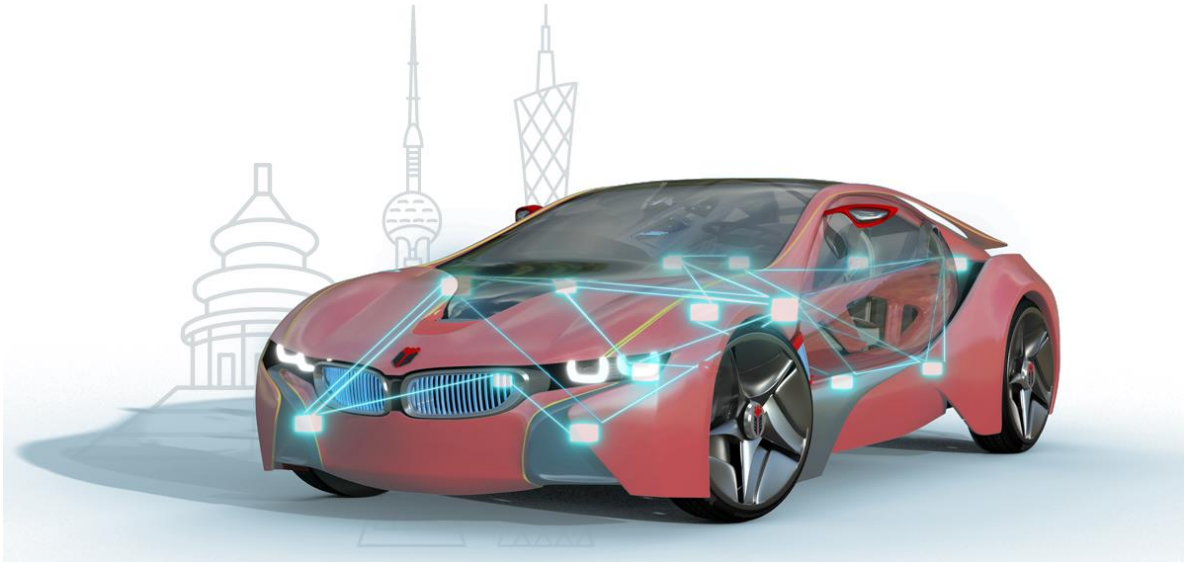
知从啸天信息安全算法产品手册

ZC.XIAOTIAN CYBER SECURITY ALGORITHM TOOLS

知从啸天工具

ZC.XiaoTian Tool



知从啸天信息安全算法产品手册

ZC.XIAOTIAN CYBER SECURITY ALGORITHM TOOLS

知从啸天工具

ZC.XiaoTian Tool

1 功能概述 FUNCTIONAL OVERVIEW

啸天信息安全算法工具是一款专为汽车行业信息安全开发的综合性密码学工具套件。在汽车智能化和网联化快速发展的背景下，车载系统的信息安全已成为汽车电子开发的核心关注点。本工具针对汽车 ECU 固件加密与签名验证、车载通信安全密钥管理、符合 AUTOSAR 标准的密码学操作等实际应用场景，为汽车信息安全工程师提供了一站式的密码学操作平台。

ZC Xiaotian Cyber Security Algorithm Tool is a comprehensive cryptographic tool suite developed specifically for Cyber Security in the automotive industry.Against the backdrop of the rapid development of automotive intelligentization and connectivity, Cyber Security of in-vehicle systems has become a core focus in automotive electronics development.Targeting practical application scenarios such as automotive ECU firmware encryption and signature verification, in-vehicle communication security key management, and cryptographic operations compliant with the AUTOSAR standard, this tool provides automotive Cyber Security engineers with a one-stop cryptographic operation platform.

2 应用领域 APPLICATION FIELD

知从啸天信息安全算法工具供信息安全算法工程师使用，可以用于开发、测试及产线。

Xiaotian Cyber Security Algorithm Tools is designed for Cyber Security algorithm engineers and applicable to development, testing, and production lines.

- 研发: 用于算法接口调试与验证

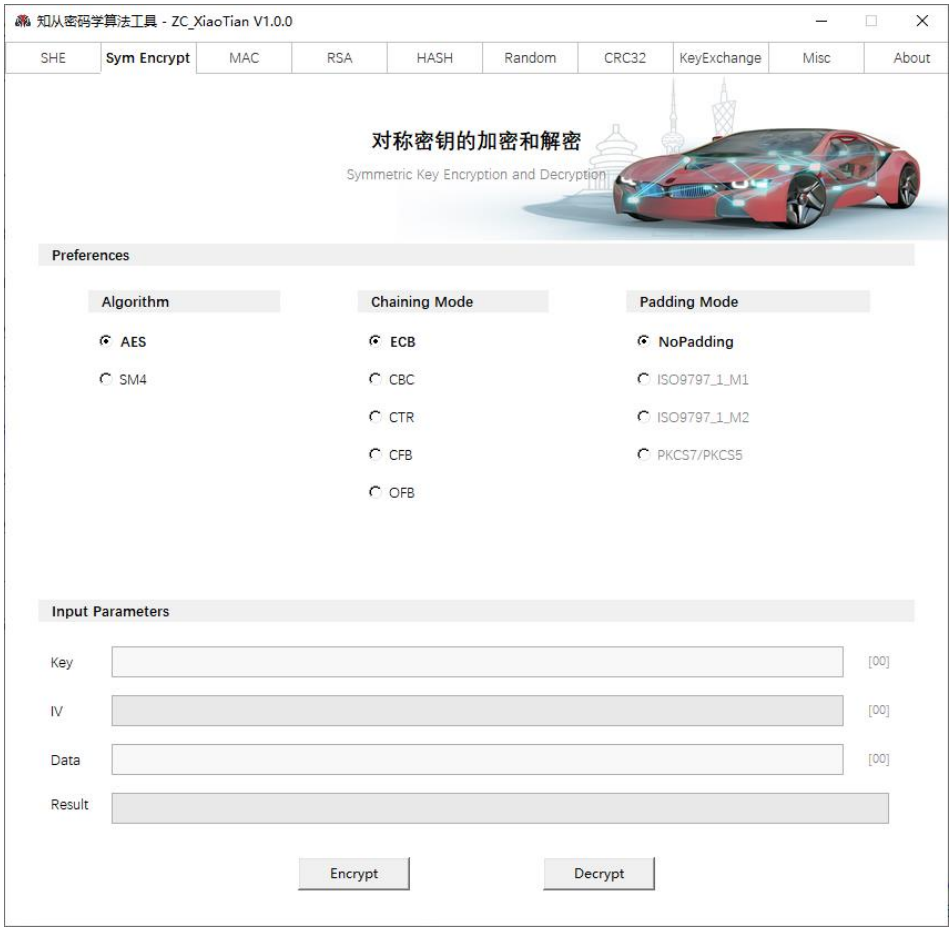
R&D: Used for algorithm interface debugging and verification.

- 测试: 提供丰富 API 接口,实现算法自动化测试

Testing: Provides rich API interfaces to enable automated algorithm testing.

- 产线: 支持产线上位机调用 api 接口,可实现密钥灌装,安全升级等,实现产线自动化

Production Lines: Supports API interface calls by production line host computers, enabling functions such as key injection and secure upgrades to achieve production line automation.



3 配置环境 CONFIGURATION ENVIRONMENT

配置环境 Configuration Environment	
Configuration Environment	Win10/11 64bit

4 开发背景 DEVELOPMENT BACKGROUND

随着汽车产业智能化、网联化转型的加速推进，车载系统不再是孤立的电子控制单元集合，而是逐渐演变为高度互联、数据密集的智能终端。这一变革在提升驾驶体验与出行效率的同时，也使车载系统面临的信息安全风险显著加剧 ——ECU 固件被篡改、车载通信数据被窃取、密钥管理混乱等安全隐患，不仅可能导致车辆功能异常，更直接威胁驾乘人员的生命财产安全。因此，车载信息安全已从可选需求转变为汽车电子开发的核心硬性指标，成为行业竞争与合规落地的关键考量。

With the accelerated transformation of the automotive industry towards intelligentization and connectivity, in-vehicle systems are no longer a collection of isolated electronic control units (ECUs) but have gradually evolved into highly interconnected and data-intensive intelligent terminals. While this transformation enhances driving experience and travel efficiency, it also significantly intensifies the Cyber Security risks faced by in-vehicle systems — security hazards such as tampering with ECU firmware, theft of in-vehicle communication data, and chaotic key management may not only cause abnormal vehicle functions but also directly threaten the life and property safety of drivers and passengers. Therefore, in-vehicle Cyber Security has shifted from an optional requirement to a core mandatory indicator in automotive electronics development, becoming a key consideration for industry competition and compliance implementation.

然而，当前市场上的密码学工具多为通用型产品，缺乏对汽车行业应用场景的针对性适配：要么无法满足 ECU 固件加密与签名验证、车载通信密钥全生命周期管理等特定需求，要么不兼容 AUTOSAR 等汽车行业核心技术标准，导致信息安全工程师需整合多款工具完成开发工作，存在操作分散、流程繁琐、兼容性差等问题，严重影响开发效率与安全防护的一致性。

However, most cryptographic tools currently available on the market are general-purpose products, lacking targeted adaptation to the application scenarios of the automotive industry: either they fail to meet specific needs such as ECU firmware encryption and signature verification, or full-lifecycle key management for in-vehicle communications, or they are incompatible with core automotive industry technical standards like AUTOSAR. This forces Cyber Security engineers to integrate multiple tools to complete development work, leading to issues such as dispersed operations, cumbersome processes, and poor compatibility. These problems seriously affect development efficiency and the consistency of security protection.

为解决上述行业痛点，针对性填补汽车行业专用密码学工具的空白，啸天信息安全算法工具应运而生。产品聚焦汽车信息安全核心场景，以 “贴合行业需求、兼容行业标准、简化操作

流程”为核心目标，打造了一站式综合性密码学工具套件，为工程师提供从固件安全到通信安全的全流程密码学操作支持，助力汽车企业高效落地信息安全合规要求，保障智能网联汽车的安全稳定运行。

To address the aforementioned industry pain points and specifically fill the gap in dedicated cryptographic tools for the automotive industry, Xiaotian Cyber Security Algorithm Tools has emerged. Focusing on core scenarios of automotive Cyber Security, the product is built with the core objectives of "aligning with industry needs, complying with industry standards, and simplifying operational processes," creating a one-stop comprehensive cryptographic tool suite. It provides engineers with end-to-end cryptographic operation support from firmware security to communication security, helping automotive enterprises effectively implement Cyber Security compliance requirements and ensure the safe and stable operation of intelligent connected vehicles.

功能模块介绍 Introduction to Functional Modules

功能模块介绍 Introduction to Functional Modules	
模块名称 Module Name	具体描述 Detailed Description
对称加密解密 Symmetric Encryption & Decryption	支持 AES、SM4 等算法，涵盖 ECB、CBC、CFB、OFB、CTR、XTS 等多种工作模式 Supports algorithms such as AES and SM4, covering multiple operation modes including ECB, CBC, CFB, OFB, CTR, and XTS.
消息认证码(MAC) Message Authentication Code (MAC)	提供 CMAC、HMAC 等完整性校验方案，支持 AES-CMAC、SM4-CMAC 等 Provides integrity verification schemes such as CMAC and HMAC, supporting AES-CMAC, SM4-CMAC, etc.
非对称加密(RSA) Asymmetric Encryption (RSA)	支持 RSA 密钥生成、加密解密及数字签名，兼容 PKCS#1 和 PSS 填充模式 Supports RSA key generation, encryption/decryption, and digital signatures, compatible with PKCS#1 and PSS padding modes.
哈希计算 Hash Calculation	集成 SHA-256/384/512、SM3 等主流哈希算法 Integrates mainstream hash algorithms such as SHA-256/384/512 and SM3.
数字签名与验证 Digital Signature & Verification	支持 ECDSA(secp256r1/SM2P256V1)、EdDSA(Curve25519)等椭圆曲线签名算法 Supports elliptic curve signature algorithms including ECDSA (secp256r1/SM2P256V1) and EdDSA (Curve25519).
密钥交换协议 Key Exchange Protocol	实现 DH、ECDH、ECDH-SM2 等密钥协商机制 Implements key agreement mechanisms such as DH, ECDH, and ECDH-SM2.
SHE 安全模块 SHE Security Module	专为汽车 SHE(Secure Hardware Extension)标准设计的密钥更新协议支持 Designed specifically for the automotive SHE (Secure Hardware Extension) standard, providing support for key update protocols.
辅助工具 Auxiliary Tools	包含随机数生成、CRC32 校验、十六进制文件处理、Base64 编解码、ASCII/Hex 转换等实用功能 Includes practical functions such as Random Number Generation, CRC32 Check, Hex File Processing, Base64 Encoding & Decoding, and ASCII/Hex Conversion.

6 产品特点 PRODUCT FEATURE

- 操作简易 Easy to operate
  - 图形化界面，方便配置
    Graphical interface for convenient configuration
  - 支持汽车行业常用信息安全算法
    Supports commonly used Cyber Security algorithms in the automotive industry
  - 支持对 hex 文件进行操作，如自动计算 MAC/CRC 等
    Supports operations on hex files, such as automatic calculation of MAC/CRC and other values.
- 辅助功能 Auxiliary functions
  - 随机数生成
    Random Number Generation
  - 十六进制文件处理
    Hex File Processing
  - Base64 编解码
    Base64 Encoding & Decoding
  - ASCII/Hex 转换等实用功能
    ASCII/Hex Conversion

免费试用下载二维码链接