HM-ZMN-TS001 密码数据分析工具箱 V2

产品白皮书

2025 年 12 月

北京豪密科技有限公司

目录

本产品适用于密评机构开展商用密码应用安全性评估、商用密码应用单位自查和密评从业人员培训。

1 产品功能

产品架构如下图所示：

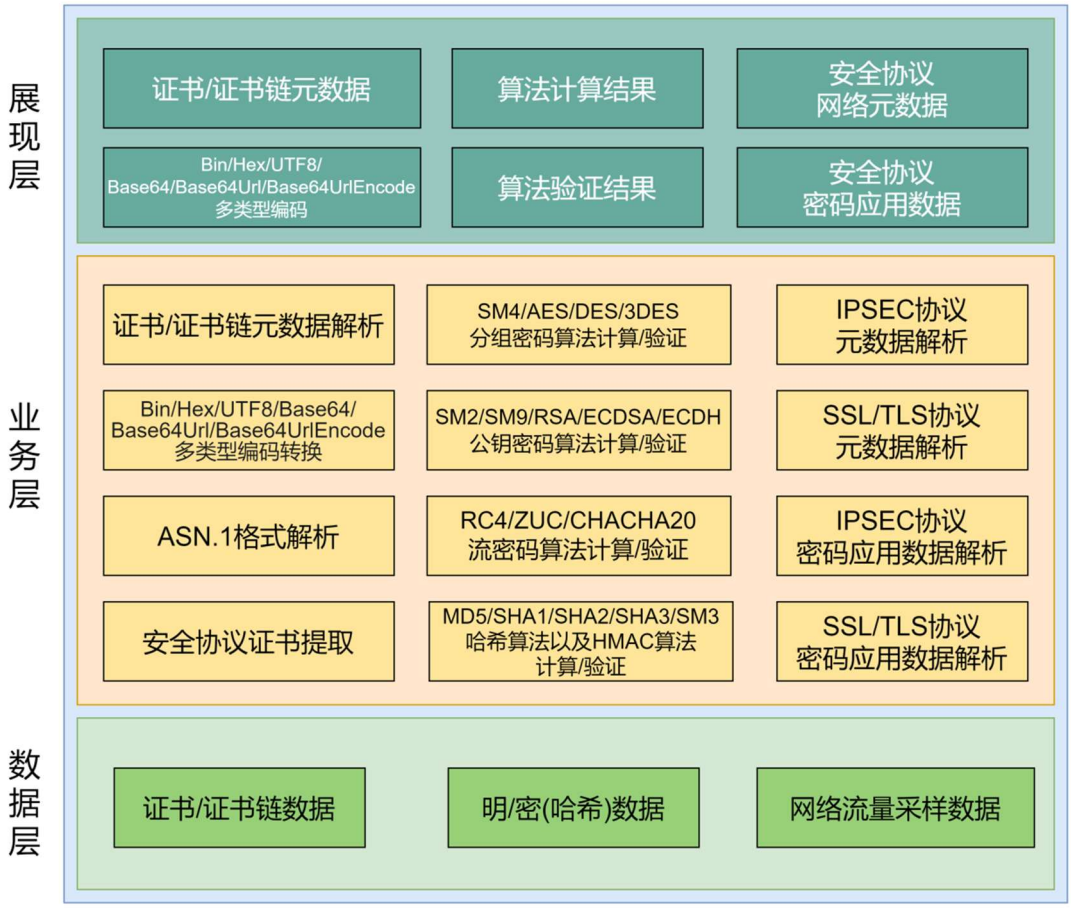

图 1 产品架构组成图

1.1 密码算法及验证工具

支持主流密码加解密运算和算法验证。

1) 分组密码算法：支持 SM4、AES、DES、3DES；

2) 公钥算法：支持 SM2、SM9、RSA（1024/2048/3072）、ECDSA、ECDH；

3) 流密码算法：支持 RC4、ZUC、ChaCha20；

4) 哈希算法：支持 MD5、SHA1、SHA2 系列、SHA3 系列和 SM3，SHA-512/224,SHA-512/256 等 13 种哈希算法以及对应的 HMAC 算法。

5) 密钥交换：支持 SM2,SM9 的密钥生成与交换，SM2 的公钥验证，SM9 的密钥封装解封。

6) MAC 算法校验：支持 MAC 算法校验功能（包括 CBC-MAC、EMAC、ANSI retail MAC、MacDES、CMAC、LMAC、TrCBC 等算法）、基于泛杂凑函数的 MAC 算法（包括 GMAC 等算法）。

密码算法及验证操作界面如下图所示：


哈希算法
HMAC
签名/验签
AES
DES
3DES
RC4
CHACHA20
SM2
SM3
SM4
ZUC
RSA
SM9
ECDH
哈希算法支持的算法有：MD4、MD5、SHA1、SHA224、SHA256、SHA384、SHA512、SHA3-224、SHA3-256、SHA3-384、SHA3-512、RIPEMD160、SM3
清空页面数据
* 明文
HEX
UTF-8
12aa12bb
迭代次数
1
盐值
HEX
UTF-8
123456
盐值位置
前加盐
转换 ↓
结果
HEX
UTF-8
Base64
md4
2d287fd0316922858729d2720de0f498
复制内容
md5
8f86c3231234282b26c29546d4923b76
复制内容
sha1
0413410492a330d10f9afa3acaf2b7d53d77d3d2
复制内容

图 2 密码算法工具


验证通过
清空页面数据
哈希算法
HMAC
AES
DES
3DES
RC4
IACHA20
SM2
SM3
SM4
ZUC
RSA
SM9
ECDH
* 明文
HEX
UTF-8
12aa12bb
哈希算法
MD5
迭代次数
1
盐值
HEX
UTF-8
123456
盐值位置
前加盐
待验证结果类型
HEX
Base64
待验证结果
文本
文件
8f86c3231234282b26c29546d4923b76
结果校验 ↓

图 3 密码算法验证工具

图 4 对称加密填充模式

1.2 签名/验签工具

支持 PKCS#1、PKCS#7 两种加密消息语法标准的签名和验签操作，识别常用编码的数据输入，支持以常用编码类型输出数据的展示形式。

PKCS#1 的签名/验签操作界面如图。支持多种非对称密码算法方案，包括：SM2、ECDSA、DSA、RSA PKCS1_V1.5、RSA PKCS1_PSS；支持多种哈希算法，包括：SM3、MD5、SHA1、SHA224、SHA256、SHA384、SHA512；支持自定义 UserID（SM2 方案）；支持 Hash(Za||M) 阶段的消息（SM2 方案）；

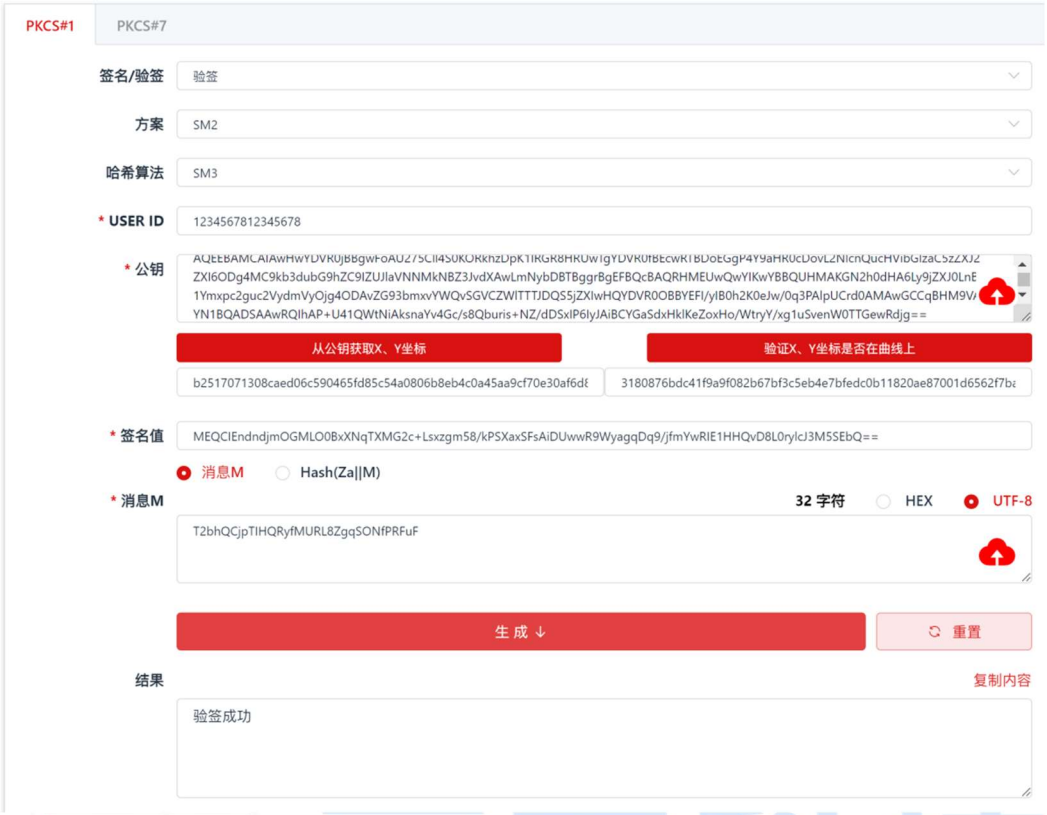

图 5 PKCS#1 操作界面

PKCS#7 的签名/验签操作界面见图。支持设置附加认证属性；支持附加多个私钥证书对；支持设置 ATTACH、DEATTACH 模式。

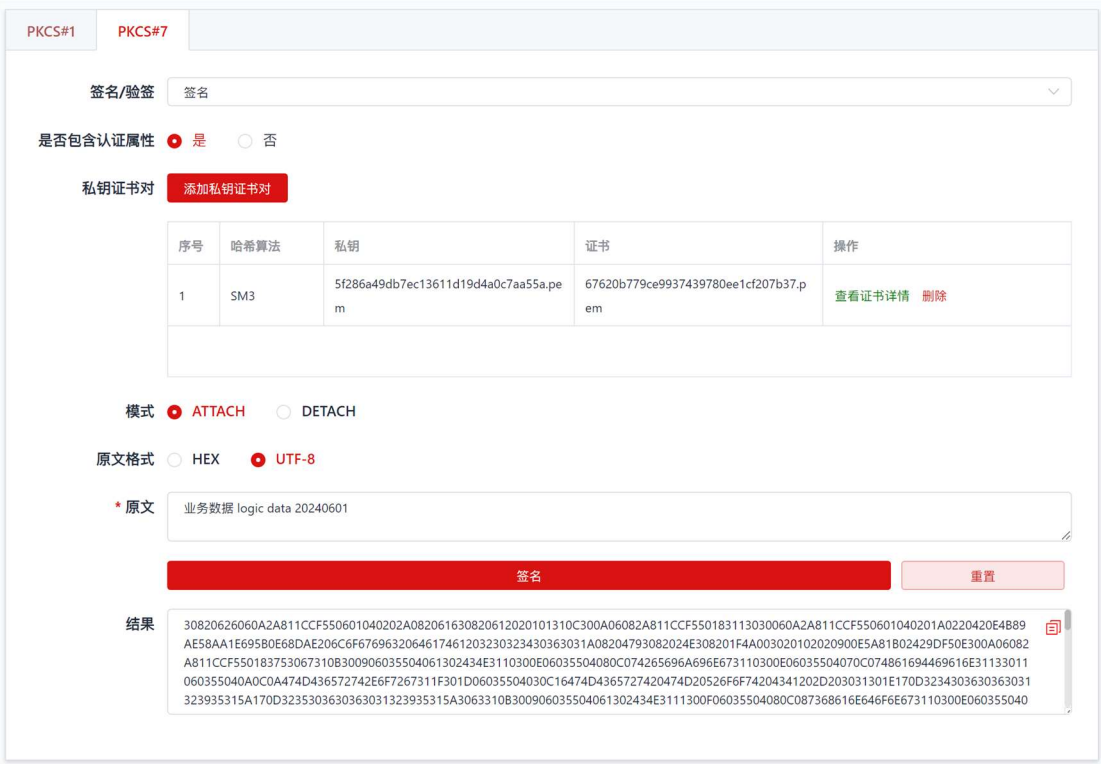

图 6 PKCS#7 操作界面

验签时除给出验签结论外，支持查看详细验签信息，提供全方位的信息展示。

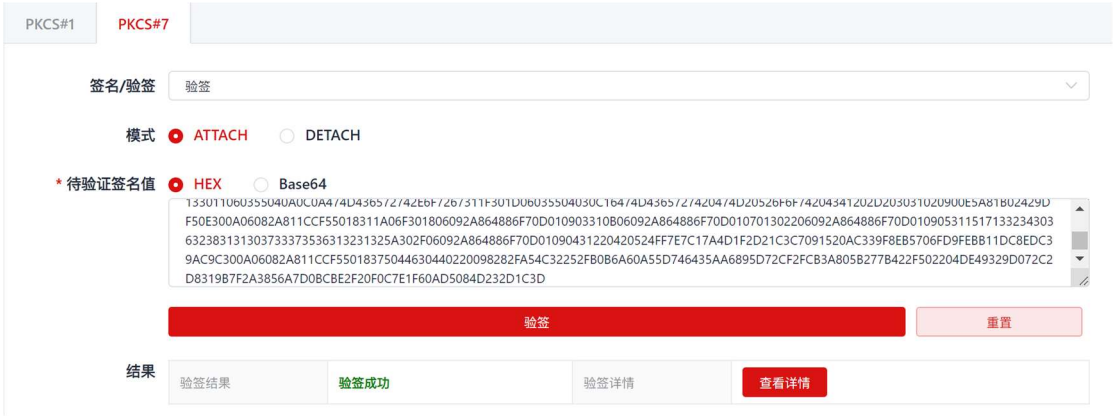

图 7 PKCS#7 验签界面

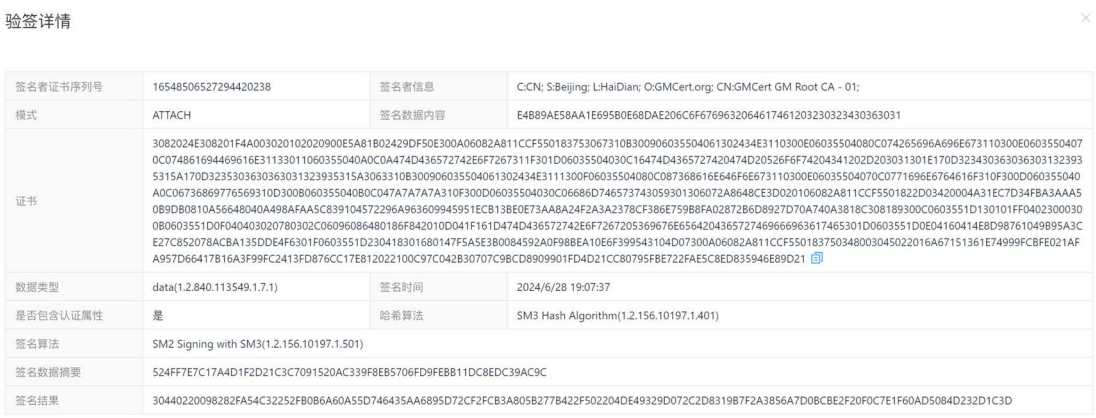

图 8 PKCS#7 验签详情

1.3 编码转换工具

支持多个编码之间，包括：HEX、UTF8、Base64、Base64URL、Base64+Url 编码之间的内容转换，如下图所示：

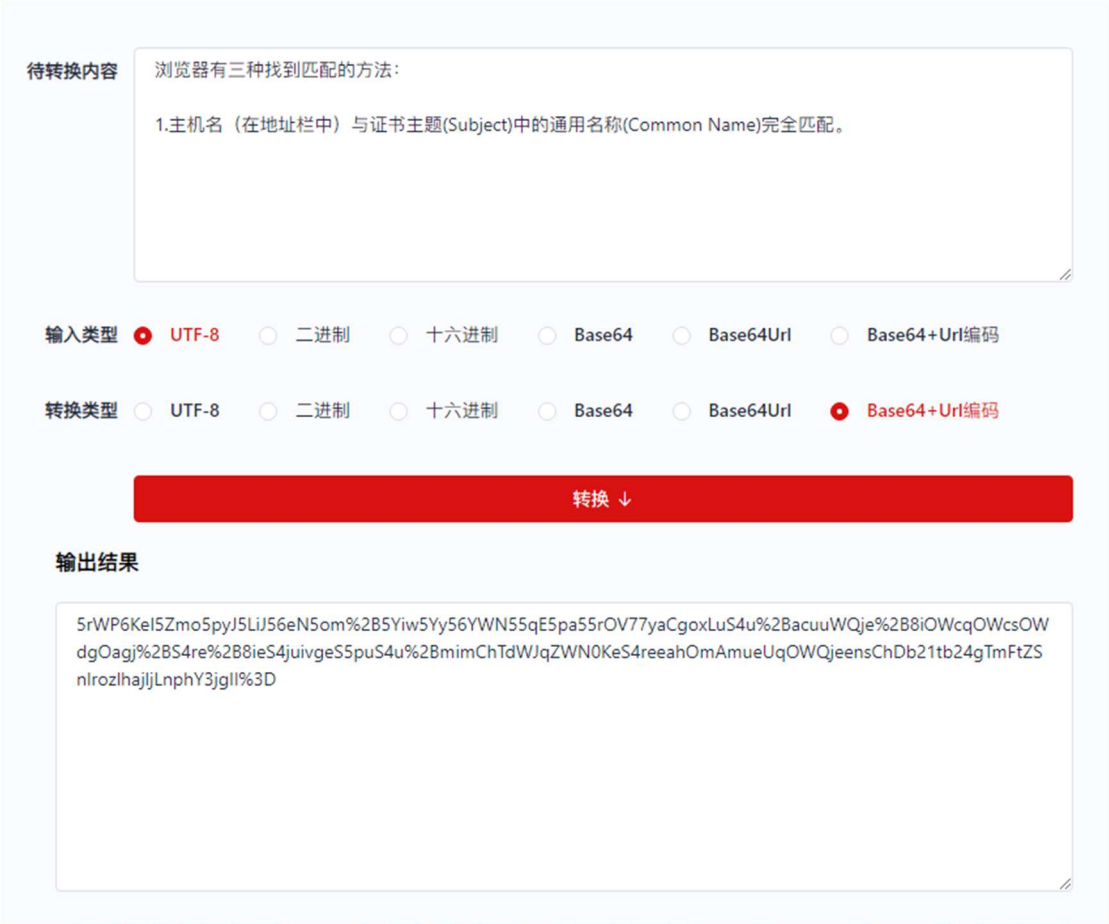

图 9 编码转换

1.4 协议分析工具

支持对常见加密协议的分析，包括国际/国密 IPSec、国际/国密 SSL/TLS（TLCP）、安全外壳协议 SSHv1、SSHv2。操作界面如下图所示：

图 10 网络流量数据协议解析

图 11 网络流量数据协议解析详情

1.5 证书分析工具

支持证书分析，并展示证书中重要字段，如证书序列号、签名算法、公钥、有效期等。

支持展示密码应用相关的重要证书元数据：

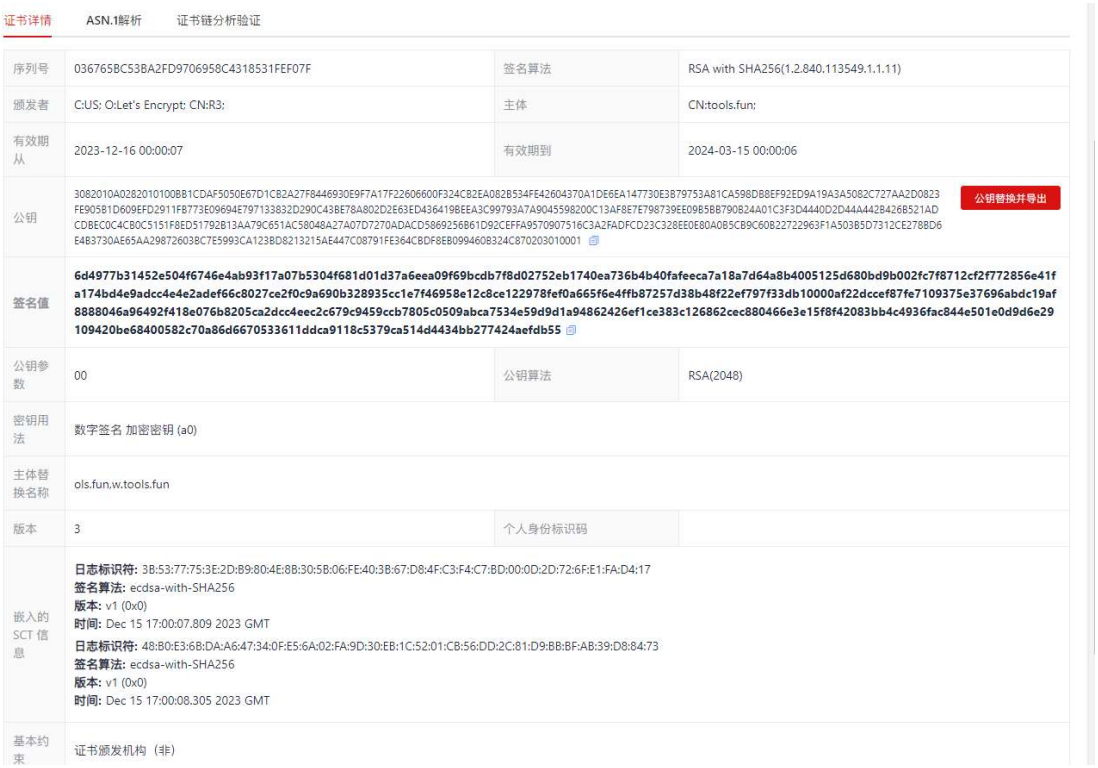

图 12 证书详情

支持解析 ASN.1 格式数据。ASN.1 解析采取结构化数据和原始数据字节比照的方式，兼顾了查看数据结构和查看源数据的两种需求。

图 13 ASN.1 格式解析

支持利用宿主的证书库以及上传的多个证书自动组链，对证书链进行验签和有效性验证，提供清晰、易于查看的界面展示，显示

分析、验签和验证的结果。

图 14 证书链分析验证

1.6 ASN.1 解析工具

支持解析 ASN.1 编码文件或数据。支持文件导入，也支持复制粘贴字符串数值；能够一键解析，获取完整详细的 ASN.1 结构树。同时，支持 XML 格式展示。

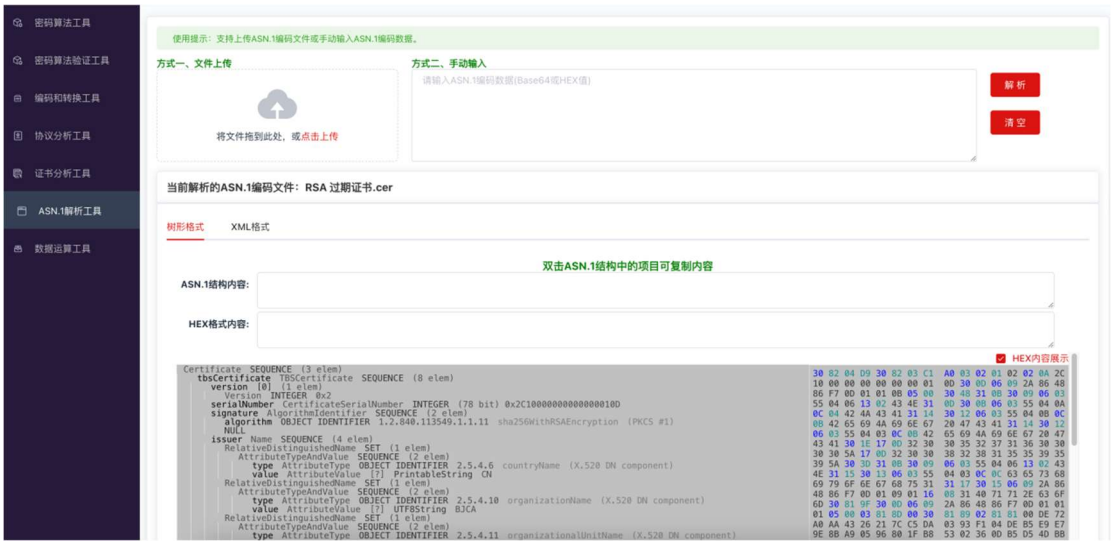

图 15 ASN.1 数据解析

在 ASN.1 结构树中双击项目，可快速复制项目值到剪切板，并

显示在结构树上方的文本框中。工具支持对比查看 HEX 数据及复制。

图 16 ASN.1 数据复制

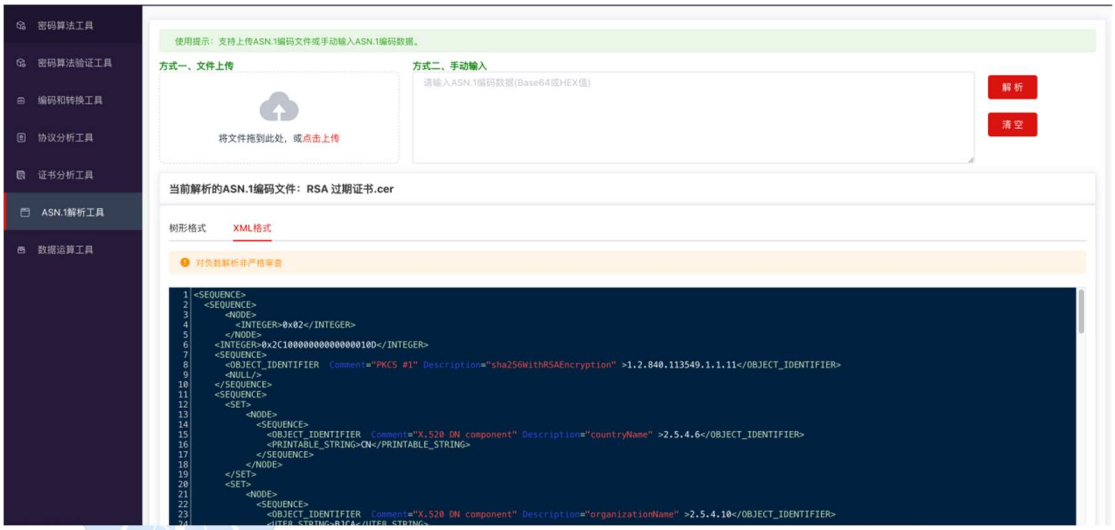

图 17 XML 展示

1.7 数据运算工具

支持大数运算，包括大数加减乘除、模逆、幂、模幂运算等；支持数据流的异或运算；支持签名验签过程中的倍点运算。

图 18 大数运算

图 19 异或运算

1.8 量化评估工具

提供符合《商用密码应用安全性评估量化评估规则（2023版）》的量化评估评分计算器，见下图所示。支持根据等保等级自动设定和展示测评指标；支持对物理和环境、网络和通信、设备和计算、应用和数据、管理制度、人员管理、建设运行、应急处置等8个安全层面，开展包含测评单元适用/不适用判定、测评对象设置、测评对象DAK打分、测评单元和安全层面综合得分自动算分等处理（可展示数据代入计算公式后的计算过程）；依照密评工作实际开展所需，在应用和数据安全层面，支持设定身份鉴别、重要数据和不可否认性指标的子测评对象；支持设定新版量化评估计算规则要求的 R_a、R_k 值，提供模拟计算功能。

图 20 量化评估计算主界面

图 21 量化评估计算过程展示

图 22 重要业务系统测评对象以及子对象

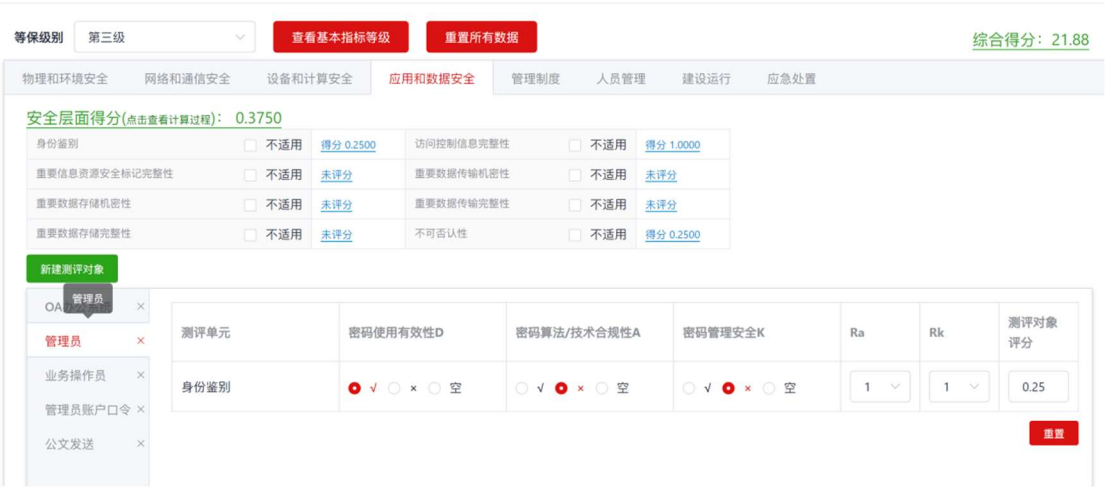

图 23 应用与数据安全层面 DAK 打分

1.9 随机性检测工具

依据 GM/T 0005-2021 《随机性检测规范》开展对输入数据和二进制密文数据的随机性检测，支持单比特频数检测、块内频数检测、扑克检测、重叠子序列检测、游程总数检测、游程分布检测、块内最大“1”游程检测、二元推导检测、自相关检测、矩阵秩检测、累加和检测等多种检测方法。

图 24 随机性检测工具主界面

如界面所示，支持手动输入和二进制文件两种输入模式，其中手动输入模式支持多种编码字符，包括十六进制字符、二进制字符和 Base64 编码字符。

GM/T 0005-2021 《随机性检测规范》增加了 Q_value 进行分布均匀性判定。主界面除了支持配置样本通过率判定显著性水平，还支持配置样本分布均匀性判定显著性水平。主界面提供设置指引，不需要查阅规范即可快速查阅规范给出的建议性参数，见下图：

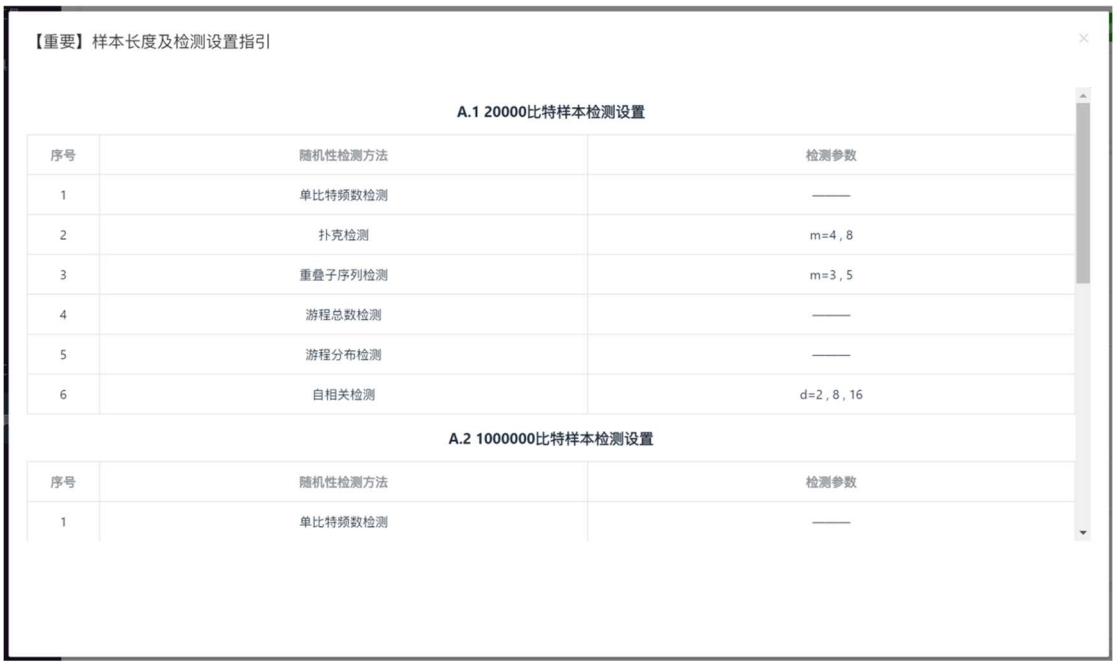

图 25 设置指引

选择随机性检测方法之后点击“开始检测”，等待计算完成后即可看到检测结果，每个被选中的方法均会获得一个样本集检测结果。见下图：

图 26 检测结果

点击“查看详情”可看到构成检测结果的详细支撑数据，见下图：

图 27 检测结果详情

2 使用方式

产品以软件方式提供，直接安装即可使用，无需连接互联网。

3 产品特点

本工具箱为单机形态软件，可在离线环境下使用，具有功能全面、系统兼容性高、简便易用等特点。

3.1 功能全面性

工具箱满足密评工作对数据分析的主要需求。数据分析涵盖密评现场测评和密评实操考核的常见数据，包含网络流量采样数据、证书/证书链数据、算法计算源数据、算法验证数据以及 ASN.1 封装文件、电子签章文件解析、随机性检测等。

工具箱可以一键解析采集的网络流量数据、证书和证书链文件，自动提取元数据及密码应用信息，开展数据完整性/机密性验证，开展对证书等 ASN.1 格式数据的分析以及有效性验证，开展密评量化

评估判别打分与分值综合计算。以友好方式分门别类呈现密评所关注的重要信息。

3.2 系统兼容性

工具箱兼容多种常见操作系统，包括：Windows7、Windows10、Windows11 等。

3.3 简便易用性

工具箱提供简便易用的用户体验。提供多样性的输入输出形式：支持手动输入，支持文件导入；输入、输出和转码均支持常见的编码方式，涵盖 HEX、PlainText、UTF-8、Base64、Base64URL、Base64+URLEncode 等。支持协议协商数据的处理，支持对业务层非标准格式数据的处理，满足用户多种需求。