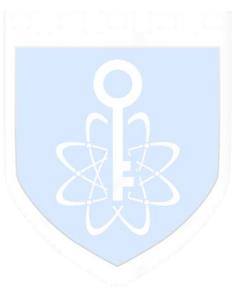


HM-ZMN-TS001

密码数据分析工具箱 V2.1

产品白皮书



豪密科技
HAOMI TECH

北京豪密科技有限公司

2024年8月

目录

| | | |
|----------|-------------|-----------|
| 1 | 产品功能 | 1 |
| 1.1 | 密码算法及验证工具 | 1 |
| 1.2 | 签名/验签工具 | 3 |
| 1.3 | 编码转换工具 | 6 |
| 1.4 | 协议分析工具 | 7 |
| 1.5 | 证书分析工具 | 7 |
| 1.6 | ASN.1 解析工具 | 9 |
| 1.7 | 数据运算工具 | 10 |
| 1.8 | 量化评估工具 | 11 |
| 1.9 | 随机性检测工具 | 13 |
| 2 | 使用方式 | 15 |
| 3 | 产品特点 | 15 |
| 3.1 | 功能全面性 | 15 |
| 3.2 | 系统兼容性 | 16 |
| 3.3 | 简便易用性 | 16 |

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：

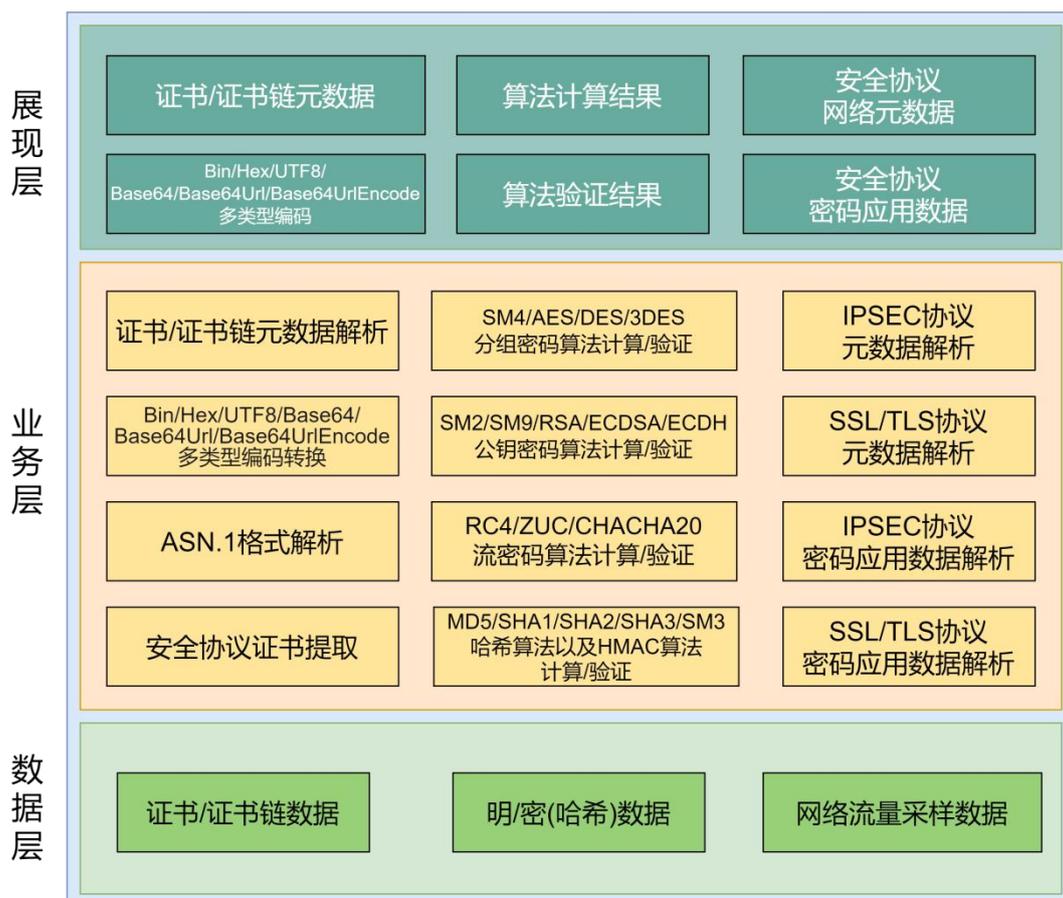


图 1 产品架构组成图

1.1 密码算法及验证工具

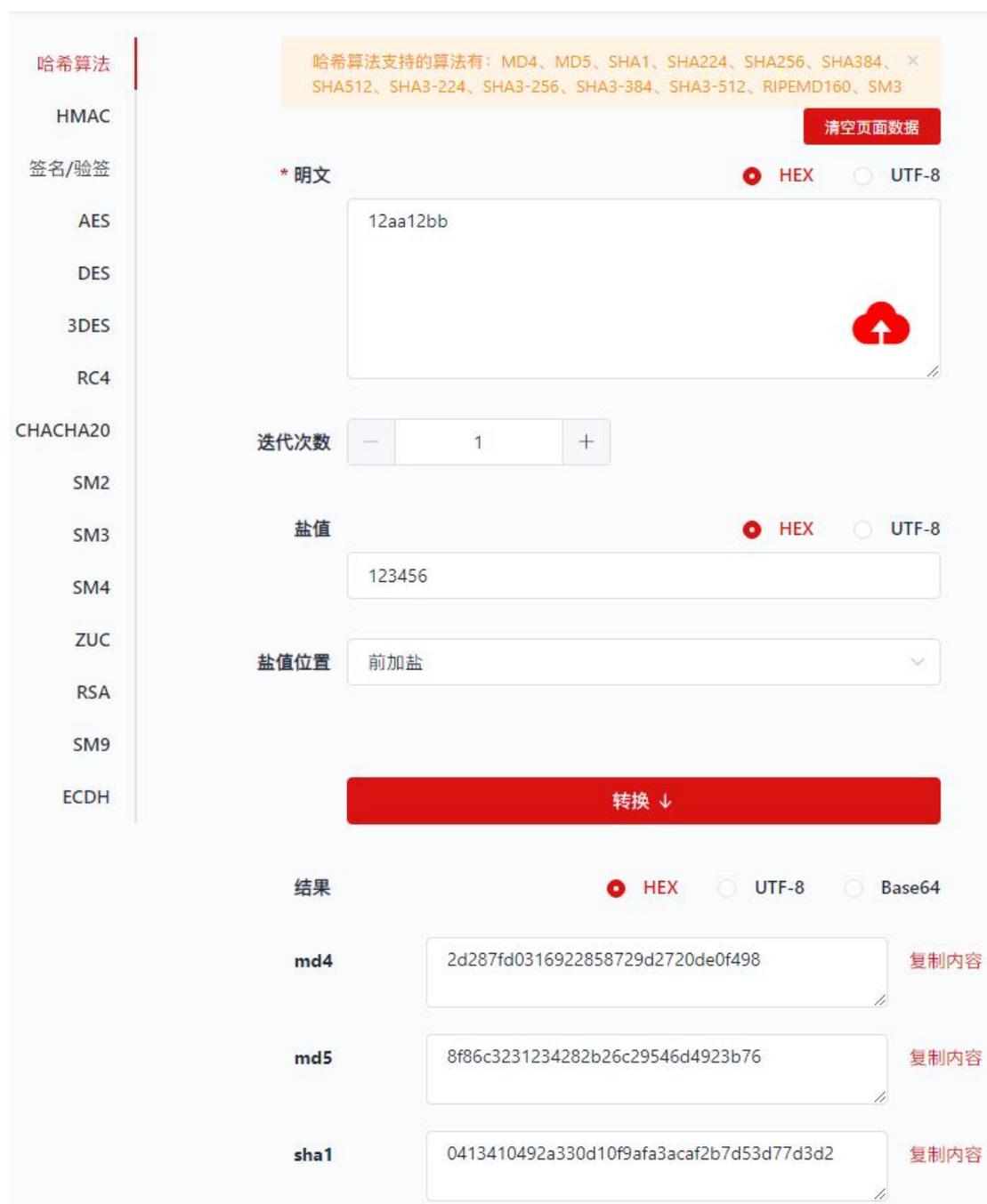
支持主流密码加解密运算和算法验证。

- 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、ECC、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 等 13 种哈希算法以及对应的 HMAC 算法。

密码算法及验证操作界面如下图所示：



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

SHA256

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

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 4。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）；

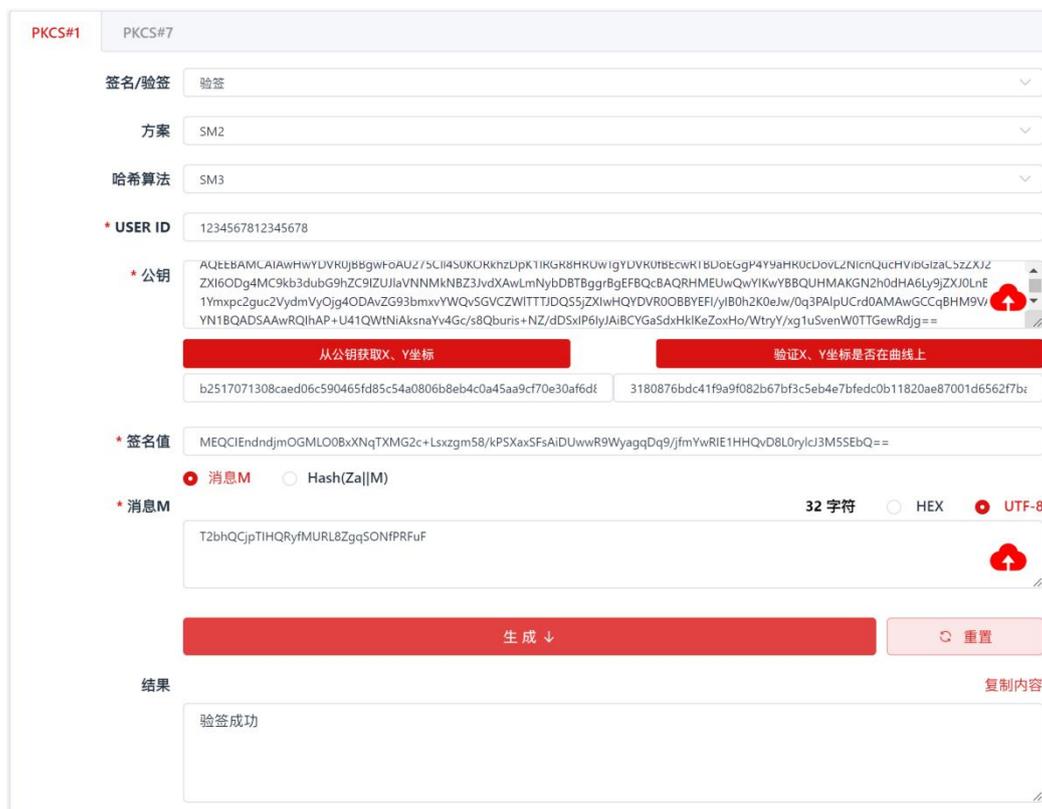


图 4 PKCS#1 操作界面

PKCS#7 的签名/验签操作界面见图 5。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。

PKCS#1
PKCS#7

签名/验签 ▼

是否包含认证属性 是 否

私钥证书对 添加私钥证书对

| 序号 | 哈希算法 | 私钥 | 证书 | 操作 |
|----|------|--------------------------------------|--------------------------------------|---|
| 1 | SM3 | 5f286a49db7ec13611d19d4a0c7aa55a.pem | 67620b779ce9937439780ee1cf207b37.pem | 查看证书详情 删除 |

模式 ATTACH DETACH

原文格式 HEX UTF-8

* 原文

签名
重置

结果

```
30820626060A2A811CCF550601040202A082061630820612020101310C300A06082A811CCF550183113030060A2A811CCF550601040201A0220420E48B9AE58AA1E69580E68DAE206C6F6769632064617461203230323430363031A08204793082024E308201F4A003020102020900E5A81B02429DF50E300A06082A811CCF550183753067310B300906035504061302434E3110300E06035504080C074265696A696E673110300E06035504070C074861694469616E31133011060355040A0C0A474D436572742E6F7267311F301D06035504030C16474D4365727420474D20526F6F74204341202D203031301E170D3234303630363031323935315A170D3235303630363031323935315A3063310B300906035504061302434E3111300F06035504080C087368616E646F6E673110300E060355040
```

图 5 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。

PKCS#1
PKCS#7

签名/验签 ▼

模式 ATTACH DETACH

* 待验证签名值 HEX Base64

```
135011060355040A0C0A474D436572742E6F7267311F301D06035504030C16474D4365727420474D20526F6F74204341202D203031020900E5A81B02429DF50E300A06082A811CCF55018311A06F301806092A864886F70D010903310B06092A864886F70D010701302206092A864886F70D010905311517133234303632383131303733373536313231325A302F06092A864886F70D01090431220420524FF7E7C17A4D1F2D21C3C7091520AC339F8EB5706FD9FEBB11DC8EDC39AC9C300A06082A811CCF55018375044630440220098282FA54C32252FB086A60A55D746435AA6895D72CF7CBA805B277B422F502204DE49329D072C2D8319B7F2A3856A7D0BCBE2F20FC7E1F60AD5084D232D1C3D
```

验签
重置

结果

| | | | |
|------|------|------|--|
| 验签结果 | 验签成功 | 验签详情 | 查看详情 |
|------|------|------|--|

图 6 PKCS#7 验签界面

验签详情

| | | | |
|----------|--|--------|--|
| 签名证书序列号 | 16548506527294420238 | 签名者信息 | C:CN; S:Beijing; L:HaiDian; O:GMCert.org; CN:GMCert GM Root CA - 01; |
| 模式 | ATTACH | 签名数据内容 | E4B89AE58AA1E69580E68DAE206C6F6769632064617461203230323430363031 |
| 证书 | 3082024E308201F44003020102020900E5A81B02429DF50E300A06082A811CCF550183753067310B300906035504061302434E3110300E06035504080C07426596A696E673110300E06035504070C074861694469616E31133011060355040ADC0A474D436572742E6F7267311F301D06035504030C16474D4365727420474D20526F6F74204341202D203031301E170D3234303630363031323935315A170D3235303630363031323935315A3063310B300906035504061302434E3111300F06035504080C087368616E646F6E673110300E06035504070C07716966E764616F310F300D060355040ADC06736869776569310D300B060355040B0C047A7A7A310F300D06035504030C06686D746573743059301306072A8648CE3D020106082A811CCF5501822D0342000AA31ECTD34F8A3AA50B9D80810A56648040A498AFAA5C839104572296A963609945951ECB138E073AA8A24F2A3A2378CF386E75988FA0287286D8927D70A740A3818C308189300C0603551D13010FF04023000300B0603551D0F040403020780302C06096086480186F842010D041F161D474D436572742E6F7267205369676E6564204365727469666963617465301D0603551D0E04160414E8D98761049895A3CE27C852078ACBA135DDE4F6301F0603551D230418301680147F5A5E3B0084592A0F98BEA10E6F399543104D07300A06082A811CCF550183750348003045022016A67151361E74999FCBF0E21AFA957D66417B16A3F99FC2413FD876CC17E812022100C97C042830707C9BC8909901FD4D21CC80795FB722FAE5C8ED835946E89D21 | | |
| 数据类型 | data(1.2.840.113549.1.7.1) | 签名时间 | 2024/6/28 19:07:37 |
| 是否包含认证属性 | 是 | 哈希算法 | SM3 Hash Algorithm(1.2.156.10197.1.401) |
| 签名算法 | SM2 Signing with SM3(1.2.156.10197.1.501) | | |
| 签名数据摘要 | 524F77EC17A4D1F2D21C3C7091520AC339F8E5706FD9FEBB11DC8EDC39AC9C | | |
| 签名结果 | 30440220098282FA54C32252F80B6A60A55D746435AA6895D72CF2FCB3A805B277B422F502204DE49329D072C2D8319B7F2A3856A7D08CBE2F20FC7E1F60AD5084D232D1C3D | | |

图 7 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：

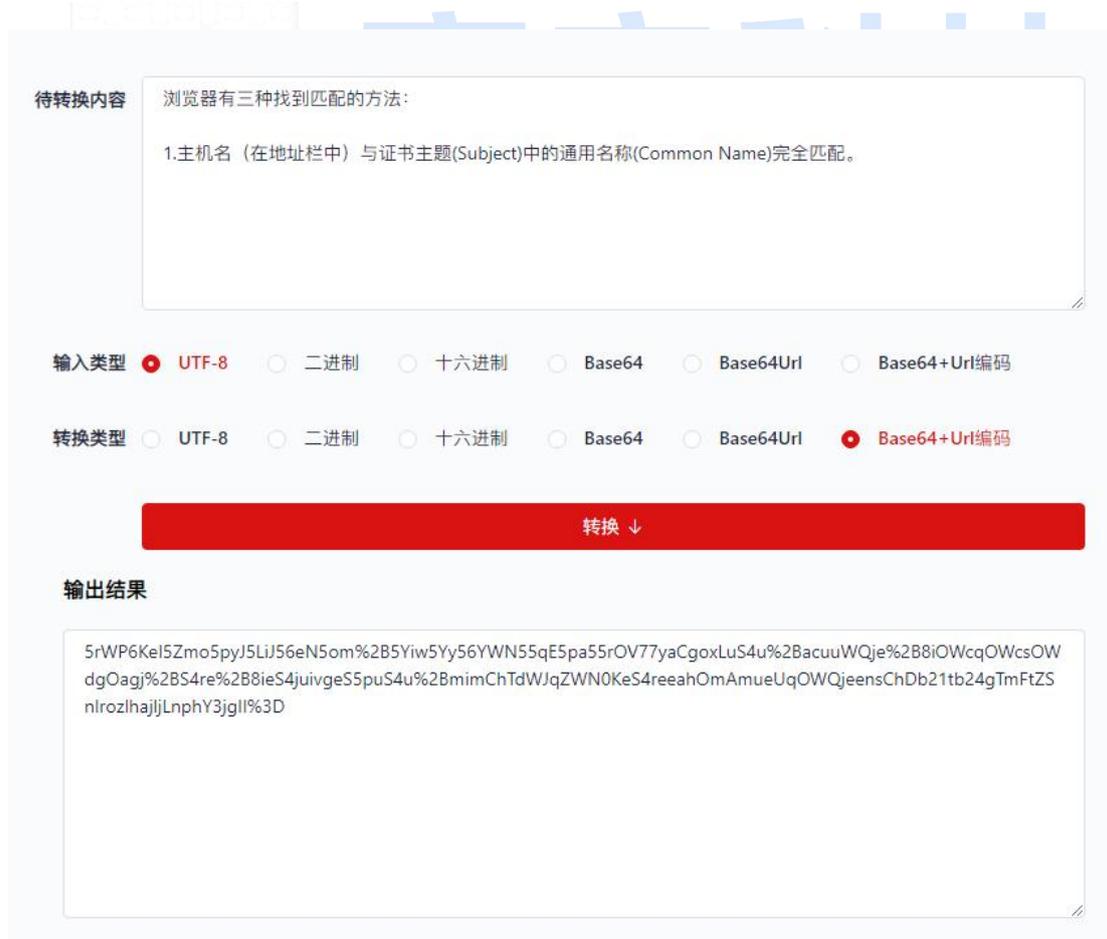


图 8 编码转换

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 9 网络流量数据协议解析



图 10 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：

| 证书详情 | ASN.1解析 | 证书链分析验证 | |
|----------|--|---------|--|
| 序列号 | 036765BC53BA2FD9706958C4318531FEF07F | 签名算法 | RSA with SHA256(1.2.840.113549.1.1.11) |
| 颁发者 | C:US; O:Let's Encrypt; CN:R3; | 主体 | CN:tools.fun; |
| 有效期从 | 2023-12-16 00:00:07 | 有效期至 | 2024-03-15 00:00:06 |
| 公钥 | 3082010A02820101008B1CDAF5050E67D1CR2A27F8446930E9F7A17F2260600F324CR2EA082B534FE42604370A1DE6EA147730E3B79753A81CA598D88EF92ED9A19A3A5062C272AA2D0823FE90581D609EFD201F8773E09694E797133832D290C43BE78A802D2E63ED436419BEFA3C99793A7A9045598200C13AF8E7E98739E09858B790824A01C3FD4440D2D444A42826B521ADCBECC0C4C80C5151F8ED51792813AA79C651AC58048A27AD07D720ADACD5869256861D92CEFFA9570907516C32AFDCD23C328EE0E80A085C89C60822722963F1A50385D7312CE2788D6E48370AE5AA298726038C7E5993CA123BD8213215AE447C08791FE364CDFE8094608324C87020310001 公钥替换并导出 | | |
| 签名值 | 6d4977b31452e504f6746e4ab93f17a07b5304f681d01d37a6eea09f69bcd7f8d02752eb1740ea736b4b40fafeeca7a18a7d64a8b4005125d680bd9b002fc7f8712cf2772856e41fa174bd4e9adcc04e4e2adef66c8027ce2f0c9a690b328935cc1e7f46958e12c8ce122978f0a665f6e4ffb87257d38b48f2ef797f33db10000af22dcecf87fe7109375e37696abdc19af8888046a96492f418e076b8205ca2dccc4ecc2c679c9459ccb7805c0509abca7534e59d9d1a94862426ef1ce383c126862cec880466e3e15f8f42083b4c493fac844e501e0d9d6e29109420be68400582c70a866d670533611ddcca9118c5379ca5114d4434bb277424aefdb55 | | |
| 公钥参数 | 00 | 公钥算法 | RSA(2048) |
| 密钥用法 | 数字签名 加密密钥 (a0) | | |
| 主体替换名称 | ols.fun,w.tools.fun | | |
| 版本 | 3 | 个人身份标识码 | |
| 嵌入的SCT信息 | 日志标识符: 38:53:77:75:3E:2D:B9:80:4E:8B:30:5B:06:FE:40:3B:67:D8:4F:C3:F4:C7:BD:00:0D:2D:72:6F:E1:FA:D4:17 签名算法: ecdsa-with-SHA256 版本: v1 (0x0) 时间: Dec 15 17:00:07.809 2023 GMT 日志标识符: 48:80:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:E8:1C:52:01:C8:56:DD:2C:81:D9:8B:BF:AB:39:D8:84:73 签名算法: ecdsa-with-SHA256 版本: v1 (0x0) 时间: Dec 15 17:00:08.305 2023 GMT | | |
| 基本约束 | 证书颁发机构 (非) | | |

图 11 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。

只支持上传cer, crt, der, pem, p7b格式的文件

将证书或证书链文件拖到此处，或点击选择文件进行上传

上传

可输入Base64、Hex格式证书数据内容直接解析

支持输入Base64、Hex格式的证书/证书链

解析

| 证书详情 | ASN.1解析 | 证书链分析验证 |
|--|---------|--|
| <pre> Certificate SEQUENCE (3 elem) tbsCertificate TBSCertificate SEQUENCE (9 elem) version [0] (1 elem) version INTEGER 0x2 serialNumber CertificateSerialNumber INTEGER (138 bit) 0x36765BC53BA2FD9706958C4318531FEF07F signature AlgorithmIdentifier SEQUENCE (2 elem) algorithm OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSASignature (PKCS #1) NULL issuer Name SEQUENCE (3 elem) RelativeDistinguishedName SET (1 elem) AttributeTypeAndValue SEQUENCE (2 elem) type AttributeType OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component) value AttributeValue [?] PrintableString US RelativeDistinguishedName SET (1 elem) AttributeTypeAndValue SEQUENCE (2 elem) type AttributeType OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component) value AttributeValue [?] PrintableString Let's Encrypt RelativeDistinguishedName SET (1 elem) AttributeTypeAndValue SEQUENCE (2 elem) </pre> | | <div style="text-align: right; color: red; font-size: small;">HEX内容展示</div> <pre> 30 82 04 F0 30 82 03 D8 A0 03 02 01 02 02 12 03 67 65 BC 53 BA 2F D9 70 69 58 C4 31 85 31 FE F0 7F 30 0D 06 09 2A 86 48 86 F7 0D 01 01 0B 05 00 30 32 31 08 30 09 06 03 55 04 06 13 02 55 53 31 16 30 14 06 03 55 04 0A 13 0D 4C 65 74 27 73 20 45 6E 63 72 79 70 74 31 0B 30 09 06 03 55 04 03 13 02 52 33 30 1E 17 0D 32 33 31 32 31 35 31 36 30 30 30 37 5A 17 0D 32 34 30 33 31 34 31 36 30 30 30 36 5A 30 14 31 12 30 10 06 03 55 04 03 13 09 74 6F 6F 6C 73 2E 66 75 6E 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01 00 EB IC DA F5 05 0E 67 D1 CB 2A 27 F8 44 69 30 E9 FF A1 7F 22 60 66 00 F3 24 CB 2E A0 82 B5 34 FE 42 60 43 70 A1 DE 6E A1 47 73 0E 3D 79 75 3A 81 CA 59 8D B8 EF 92 ED 9A 19 A3 A5 0E 2C 72 7A A2 D0 82 3F E9 05 </pre> |

图 12 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 13 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。

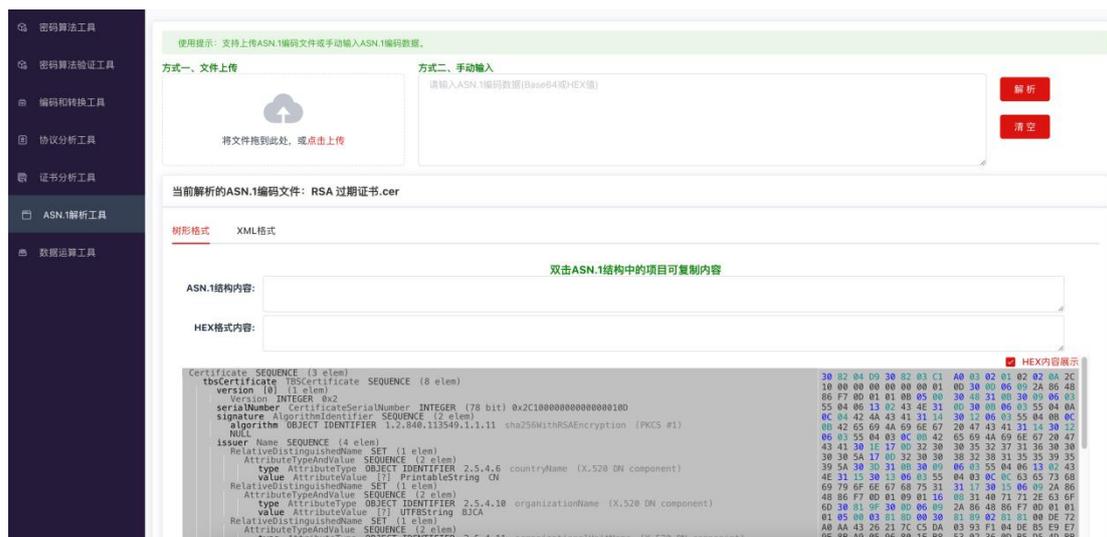


图 14 ASN.1 数据解析

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 15 ASN.1 数据复制

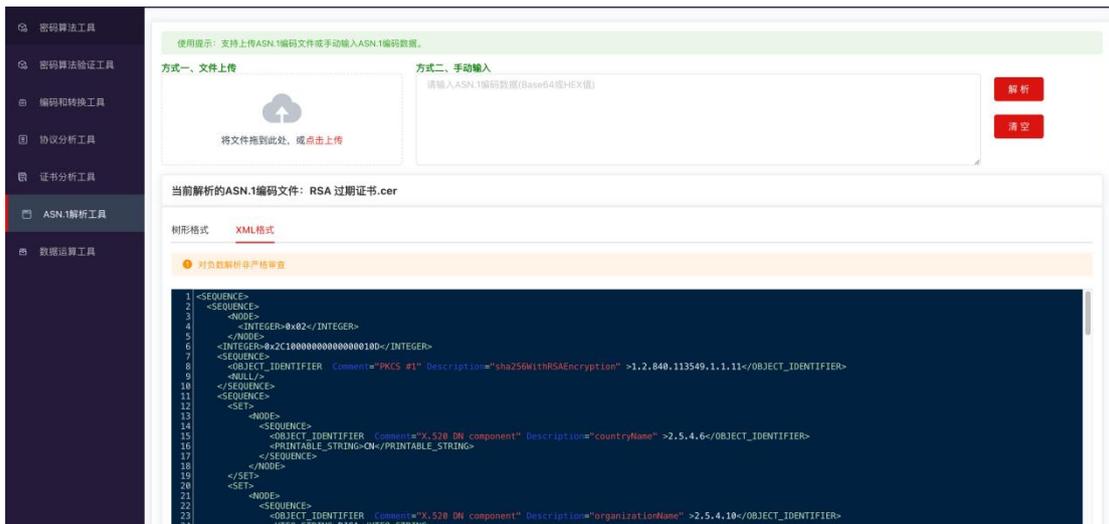


图 16 XML 展示

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。



图 17 大数运算



图 18 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 19 量化评估计算主界面



图 20 量化评估计算过程展示



图 21 重要业务系统测评对象以及子对象



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、扑克、游程分布、游程总数等多种检测方法。



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：



| A.1 20000比特样本检测设置 | | |
|-------------------|---------|------------|
| 序号 | 随机性检测方法 | 检测参数 |
| 1 | 单比特频数检测 | —— |
| 2 | 扑克检测 | m=4, 8 |
| 3 | 重叠子序列检测 | m=3, 5 |
| 4 | 游程总数检测 | —— |
| 5 | 游程分布检测 | —— |
| 6 | 自相关检测 | d=2, 8, 16 |

| A.2 1000000比特样本检测设置 | | |
|---------------------|---------|------|
| 序号 | 随机性检测方法 | 检测参数 |
| 1 | 单比特频数检测 | —— |

图 24 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：

| 单比特频数检测 | 扑克检测 | 游程总数检测 |
|--|--|---|
|  <p>检测结果: 通过 通过率判定: 通过 分布均匀性判定: 通过</p> <p>查看详情</p> |  <p>检测结果: 通过 通过率判定: 通过 分布均匀性判定: 通过</p> <p>查看详情</p> |  <p>检测结果: 通过 通过率判定: 通过 分布均匀性判定: 通过</p> <p>查看详情</p> |

图 25 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：

检测结果详情 (P_value用于样本通过率判定、Q_value用于样本分布均匀性判定)

| 样本 | 样本通过率判定 | 样本分布均匀性判定 |
|-----|--|--|
| 样本1 | P_value1 : 0.215925 检测通过 | Q_value1 : 0.892038 pT: 0.437274 检测通过 |

图 26 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。

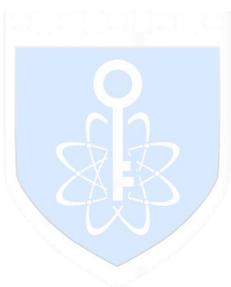
工具箱可以一键解析采集的网络流量数据、证书和证书链文件，自动提取元数据及密码应用信息，开展数据完整性/机密性验证，开展对证书等 ASN.1 格式数据的分析以及有效性验证，开展密评量化评估判别打分与分值综合计算。以友好方式分门别类呈现密评所关注的重要信息。

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。



豪密科技
HAOMI TECH