WiAuth

一个简化授权的小东西~

网络技术文档

BY 小傅Fox

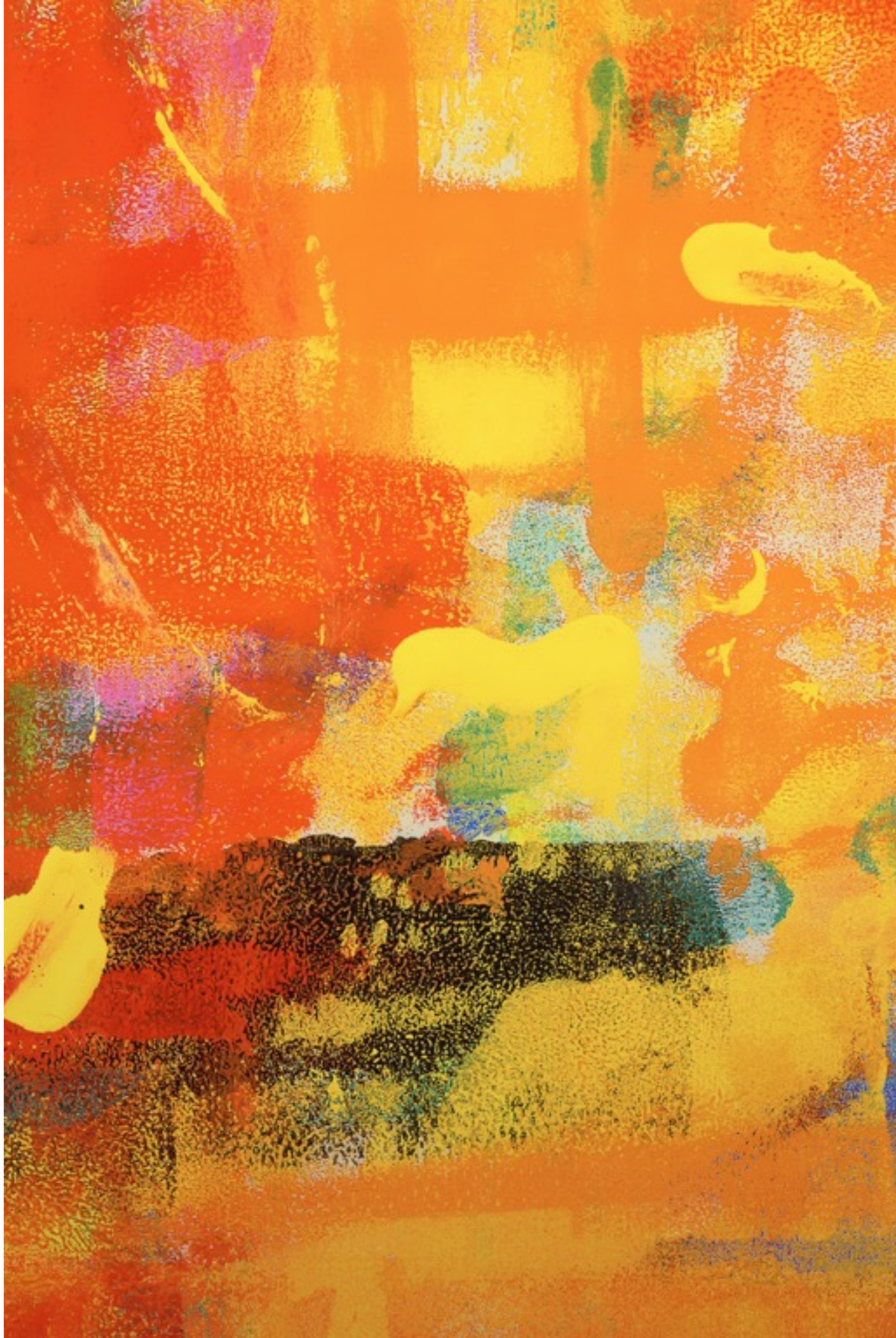
加密

ENCRYPTING

RSA算法

- 适用范围：所有数据包
- 密钥保存：固化（电脑端与手机端不同）
- 错误处理：解密内容无意义则丢弃
- 问题：速度

数据流程



手机端广播

- 数据协议：UDP
- 方式：广播
- 加密方式：RSA

- 明文：UID
- 端口：49160（待定）
- 时间间隔：60s（待定）

示例

- UDP:Server 192.168.1.2
- Broadcast: 192.168.1.1~192.168.1.255:49160
- Data:
  00001
- 解释:
  手机端IP 192.168.1.2
  用户UID 1（编码为6位定长数字）

计算机配对

- 数据协议：TCP
- 端口：49161
- 连接发起方：计算机
- 过程1：计算机发送key
- 过程2：手机回应校验结果

过程1数据包

- 发送者：计算机
- 内容：
  “PAIR”+key
- 示例：
  192.168.1.3:49161 - - > > 192.168.1.2:49161
  PAIR1234
- 解释：key为四位数字
- 注：“PAIR”具体内容可另行商定

过程2数据包

- 发送者：手机
- 内容：
  “PAIROK”+key
- 示例：
  192.168.1.2:49161 - - > > 192.168.1.3:49161
  PAIROK1234
- 注：“PAIROK”具体内容可另行商定

授权请求

- 数据协议：TCP
- 端口：49161
- 连接发起方：计算机
- 过程1：计算机表示授权请求
- 过程2：手机反馈token

过程1数据包

- 发送者：计算机
- 内容：
  “AUTH”+key+请求UUID
- 示例：
  192.168.1.3:49161 - - > > 192.168.1.2:49161
  AUTH123401
- 解释：key为四位数字，UUID为两位数字
- 注：“AUTH”具体内容可另行商定

过程2（授权成功）数据包

- 发送者：手机
- 内容：
  “AUTHOK”+token
- 示例：
  192.168.1.2:49161 - - > > 192.168.1.3:49161
  AUTHOK9975410663 3f94d350db34d548d6091a
- 注：“AUTHOK”具体内容可另行商定，token的格式需要在开发时共同确定，前期可以使用本例内容代替

过程2（授权失败）数据包

- 发送者：手机
- 内容：
  “AUTHFAIL”+错误码
- 示例：
  192.168.1.2:49161 - - > > 192.168.1.3:49161
  AUTHFAIL01
- 注：“AUTHFAIL”具体内容可另行商定，错误码另表，为两位数字

错误类型表

- 01 用户拒绝授权
- 02 用户修改了配对密码
- 03 远程服务器错误
- 04 其它错误