# 密码算法简介

罗鹏

中国科学院信息工程研究所

2017.01.01

#### 大纲

- ▶ 对称密码算法 (私钥密码算法)
  - ▶ 分组密码 (Block Cipher)
  - ▶ 流密码 (Stream Cipher)
  - ▶ 工作模式 (Mode of Operation)
  - ▶ 密码杂凑函数 (Hash Function)
  - ▶ 消息认证码 (Message Authentication Code)
  - ▶ 认证加密 (Authenticated Encryption)
- ▶ 非对称密码算法 (公钥密码算法)
  - ▶ 密钥交换算法 (Key Exchange)
  - ▶ 公钥加密 (Public-Key Encryption)
  - ▶ 数字签名 (Digital Signature Algorithm)

**幼椒椒**椒 浓嫩的 工作结单 原则丸填不断 消息计算的 计算标数 原积六极管计 从积标束管计 新安装存

### 分组密码 (Block Cipher)

#### 经典分组密码

- DES
- ► AES
- Serpent
- Twofish
- ► SM4
- ► RC6
- ▶ GOST
- **>** ...

#### 轻量级分组密码

- ► HIGHT
- ▶ PRESENT
- LBlock
- ▶ PRINCE
- ► RECTANGLE
- ► SIMON
- ► SKINNY

公何变现 海療理 工作信护 原现办法活路 出自江江亚 江江和家 原组亦植管注 小组和家管注 斯安茨克

# 流密码 (Stream Cipher)

- ► RC4
- ► Salsa20
- ChaCha
- ▶ ..

**分组密码 连密码 工作模式** 密码杂凑通数 消息认证码 认证加密 密钥交换算法 公钥加密算法 数字签名

# 工作模式 (Mode of Operation)

- ► ECB
- ► CBC
- ► CFB
- ► OFB
- ► CTR

分组密码 笼密码 工作模式 密码杂凑函数 消息认证码 钛证加密 密钥交换算法 公钥加密算法 数字签名

### 密码杂凑函数 (Hash Function)

- ► MD5
- ► SHA1
- ► SHA2
- ► SHA3
- ► BLAKE2
- ▶ Grøstl
- ► JH
- ► SM3
- **.**..

分组密码 笼密码 工作模式 密码杂凑函数 消息认证码 松订加密 密钥交换算法 公钥加密算法 数字签名

### 消息认证码 (Message Authentication Code)

- ► CBC-MAC
- ► HMAC
- OMAC
- ► Poly1305
- DAA
- **.**..

分组密码 笼密码 工作模式 密码杂凑函数 消息认证码 **认证加密** 密钥交换算法 公钥加密算法 数字签名

# 认证加密 (Authenticated Encryption)

- ► CCM
- ► EAX
- ► GCM
- ▶ OCB
- **...**

#### Caesar Candidates

- ACORN
- Deoxys
- ▶ PRIMATEs
- ► SHELL
- **.**..

分组密码 法密码 工作模式 密码杂语函数 消息认证码 认证加密 **密钥交换算法** 公钥加密算法 数字答名

#### 密钥交换算法 (Key Exchange)

- ▶ Diffie-Hellman 密钥交换,简称 DH
- ▶ 基于非对称密码算法
  - Elliptic curve Diffie-Hellman (ECDH 或者 ECDHE),基于 ECC

**.**..

分组密码 渡密码 工作模式 密码杂凑函数 消息认证码 认证加密 密钥交换算法 公銷加密算法

# 公钥加密 (Public-Key Encryption)

- ► RSA
- ► ECC
- **...**

自密码 流密码 工作模式 密码杂凑函数 消息认证码 认证加密 密钥交换算法 公钥加密算法 **数字签名** 

#### 数字签名 (Digital Signature Algorithm)

数字签名都是通过非对称密码算法实现。

- ► RSA
- ▶ Elliptic Curve Digital Signature Algorithm (ECDSA),基于 ECC
- Edwards-curve Digital Signature Algorithm (EdDSA)