现代密码学

身份基密码体制

信息与软件工程学院

身份基密码体制

- 身份基密码体制背景知识
- 数学基础
- Boneh-Franklin身份基加密算法

身份基密码体制背景知识

- PKI公钥密码体制的问题
  - 发送者必须拥有接收者的证书
  - 证书管理和CRL的复杂性
  - 安全性悖论
    - 证书数据库被暴露给组织/机构

身份基密码体制背景知识

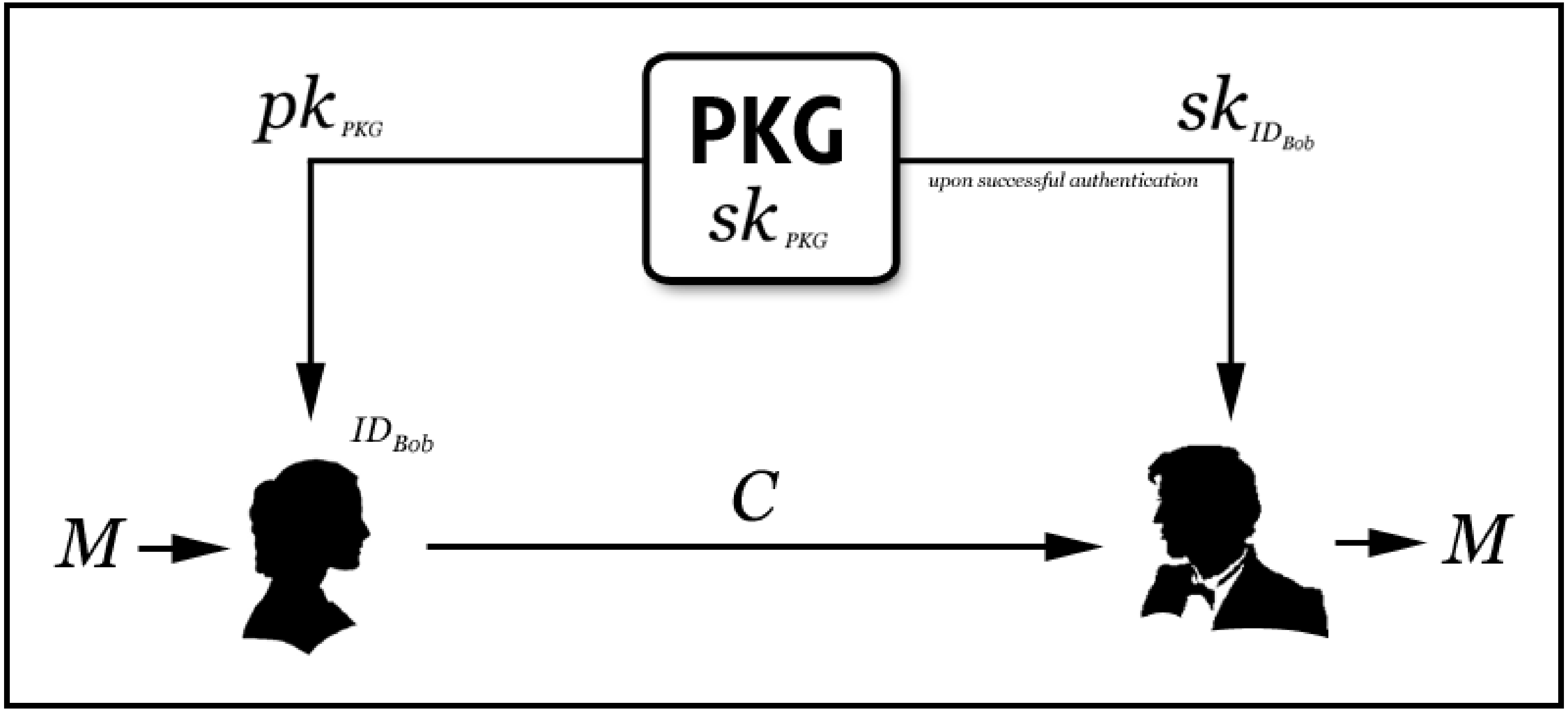
- 身份基公钥密码体制的优势
  - 针对未准备用户的密码学
  - 公钥是用户身份的某些属性，例如电子邮件地址，电话号码或生物识别数据
  - 发件者只需知道接收者的身份属性即可发送加密邮件
  - 接收者在收到加密邮件之后才需要与系统交互。

身份基密码体制背景知识

- 1984年由Shamir提出
  - Shamir提出了一个身份基签名（Identity-based signature，IBS）的工作系统，但没有提出身份基加密（Identity-based encryption，IBE）的系统
- 第一个身份基加密的系统由Boneh和Franklin在2001提出，该系统基于Weil配对
- 密码学当前热门课题

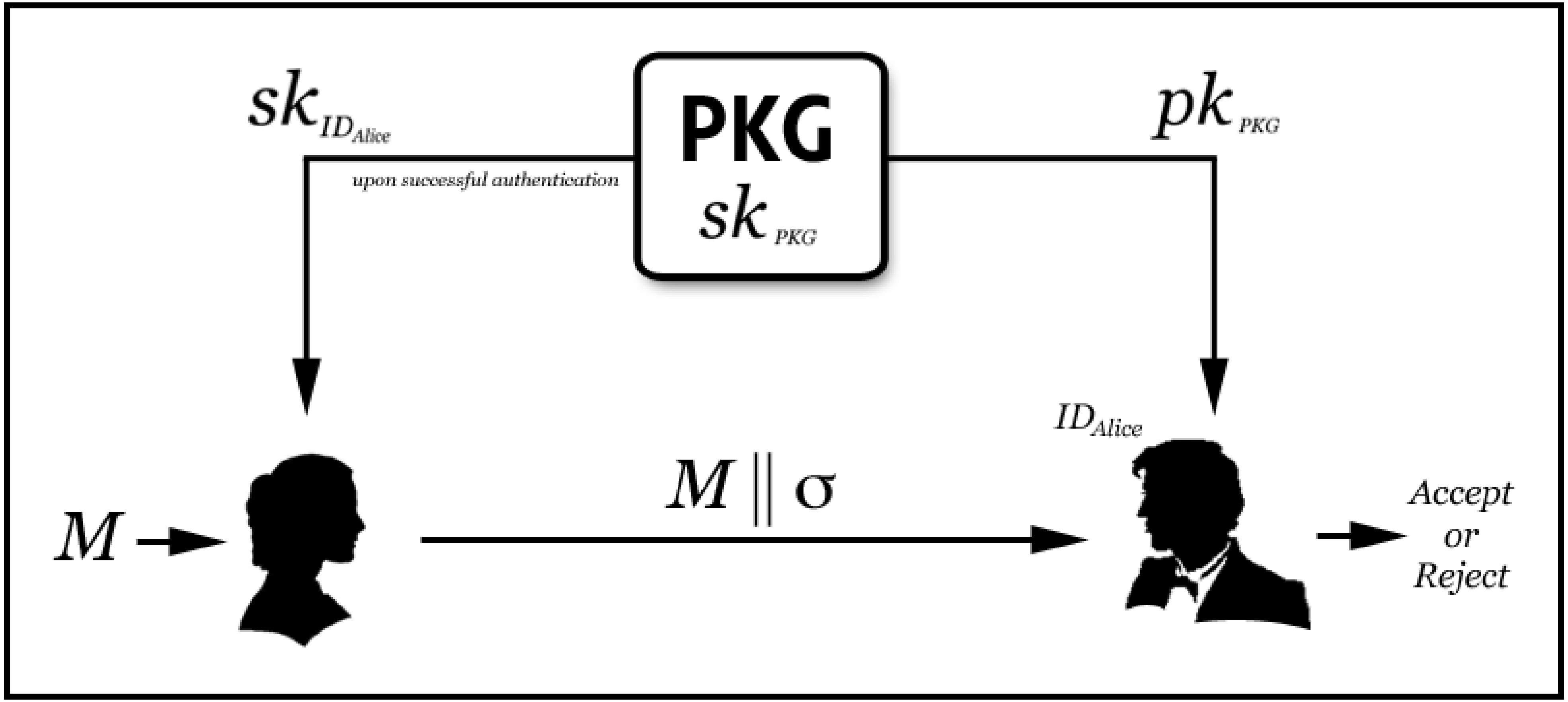
Adi Shamir: Identity-Based Cryptosystems and Signature Schemes, CRYPTO 1984: 47-53 Citations:7479
Dan Boneh, Matthew K. Franklin, Identity-Based Encryption from the Weil Pairing. CRYPTO 2001: 213-229 Citations:8336

身份基密码体制背景知识



身份基加密（IBE）

身份基密码体制背景知识



身份基签名（IBS）

Boneh-Franklin身份基加密算法

- 身份基密码体制背景知识
- 数学基础
- Boneh-Franklin身份基加密算法

数学基础

离散对数问题（Discrete Logarithm Problem）

- 对于乘法群Z_p^*，给定r,q,p，寻找整数k，使得$r = q^k \bmod p$
- 许多密码体制的基础

标量乘法（Scalar multiplication）

- $P, 2P, 3P = 2P + P, 4P = 3P + P, \ldots, kP$

椭圆曲线上的离散对数问题（ECDLP）

- 给定P, Q，寻找整数k，使得$kP = Q$

数学基础

双线性映射（Bilinear map）

- 映射 $e: G_1 \times G_1 \longrightarrow G_2$
- $\forall P, Q \in G_1, \forall a, b \in Z, e(aP, bP) = e(P, Q)^{ab}$

Weil配对（Weil Pairing）

- 双线性映射
  - G_1是椭圆曲线F_p上的点的群
  - G_2是$F_{p^2}^*$的一个子群
- 高效可计算
  - 米勒算法（Miller's algorithm）

数学基础

本文中的椭圆曲线群

- p, q是素数，$p = 2 \bmod 3$，$p = 6q - 1$
- E是由F_p上$y^2 = x^3 + 1$定义的椭圆曲线
- G_q是由$P \in E/F_p$生成的阶数$q = (p+1)/6$的群

改进的Weil配对

- $\widehat{e}: G_q \times G_q \longrightarrow \mu_q$
- μ_q是$F_{p^2}^*$的子群，包含所有的q阶元素
- 非退化：$\widehat{e}(P, P) \in F_{p^2}$是$\mu_q$的生成元

数学基础

Weil Diffie-Hellman Assumption (WDH)

- 给定$< P, aP, bP, cP >$，其中随机选择$a, b, c \in Z_q^*, P \in E/F_p$，计算$W = \widehat{e}(P, P)^{abc} \in F_{p^2}$
- 当p是随机k位素数时，不存在一个算法可以在概率多项式时间内解决WDH问题。

数学基础

MapToPoint算法

- 将任意字符串 $ID \in \{0,1\}^*$转换为一个q阶的点$Q_{ID} \in E/F_p$
- 哈希函数$G : \{0,1\}^* \longrightarrow F_p$
- 步骤：
  - $y_0 = G(ID), x_0 = (y_0^2 - 1)^{1/3}$
  - $Q = (x_0, y_0) \in E/F_p, Q_I D = 6Q$

- 无冲突
- 防篡改

身份基密码体制

- 身份基密码体制背景知识
- 数学基础
- Boneh-Franklin身份基加密算法

Boneh-Franklin身份基加密算法

初始化（Setup）：

- 使用已定义的椭圆曲线群
- 选择q阶的$P \in E/F_p$
- 选择随机$s \in Z_q^*$并设置$P_{pub} = sP$
- 选择哈希函数
  - $H : F_{p^2} \longrightarrow \{0,1\}^n$
  - $G : \{0,1\}^* \longrightarrow F_p$
- 消息空间$M = \{0,1\}^n$，密文空间为$C = E/F_p \times \{0,1\}^n$
- 系统参数是$< p, n.P, P_{pub}, G, H >$。 主密钥是$s$。

Boneh-Franklin身份基加密算法

密钥生成（Extract）：

- 使用MapToPoint将ID映射到点Q_{ID}
- 与ID对应的私钥是$d_{ID} = sQ_{ID}$

加密（Encrypt）

- 使用MapToPoint将ID映射到点Q_{ID}
- 选择随机$r \in Z_q$
- $C = < rP, M \oplus H(g_{ID}^r) >$，其中$g_{ID} = \widehat{e}(Q_{ID}, P_{pub}) \in F_{p^2}$

Boneh-Franklin身份基加密算法

解密（Decrypt $C = < U, V >$）：

- 如果 U 不是q阶的点，则拒绝密文。
- 否则，$M = V \oplus H(\widehat{e}(d_{ID}, U))$

为什么M能够被回复？

$$\widehat{e}(d_{ID}, U) = \widehat{e}(sQ_{ID}, rP) = \widehat{e}(Q_{ID}, P)^{sr} = \widehat{e}(Q_{ID}, P_{pub})^{r} = g_{ID}^{r}$$

$$V \oplus H(\widehat{e}(d_{ID}, U)) = M \oplus H(g_{ID}^{r}) \oplus H(g_{ID}^{r}) = M$$

感 谢 聆 听!

xionghu.uestc@gmail.com