八、认证加密安全
(Authenticated Encryptions)

哈尔滨工业大学

张宇

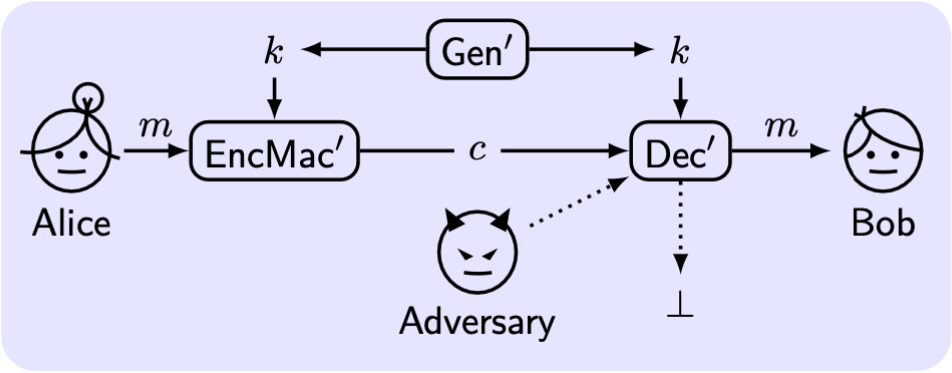
2024春

概览

1. 认证加密（Authenticated Encryptions）安全

安全消息传递

- 先不直接处理本课程中尚未解决的CCA安全，而是研究一个比CCA更安全的通信场景，其中引入了通信真实性要求，并满足CCA安全；



- **Key-generation** algorithm outputs $k \leftarrow \mathsf{Gen}'(1^n)$. $k = (k_1, k_2)$. $k_1 \leftarrow \mathsf{Gen}_E(1^n)$, $k_2 \leftarrow \mathsf{Gen}_M(1^n)$.
- **Message transmission** algorithm is derived from $\mathsf{Enc}_{k_1}(\cdot)$ and $\mathsf{Mac}_{k_2}(\cdot)$, outputs $c \leftarrow \mathsf{EncMac}'_{k_1,k_2}(m)$.
- **Decryption** algorithm is derived from $\mathsf{Dec}_{k_1}(\cdot)$ and $\mathsf{Vrfy}_{k_2}(\cdot)$, outputs $m \leftarrow \mathsf{Dec}'_{k_1,k_2}(c)$ or $\perp$.
- **Correctness requirement**: $\mathsf{Dec}'_{k_1,k_2}(\mathsf{EncMac}'_{k_1,k_2}(m)) = m$.

- 在消息传递方案中，消息被加密并且被MAC。在解密算法中，当密文没有通过真实性验证时，输出空（可以理解为“报错”）；这意味着未认证的密文无法解密。

安全认证加密

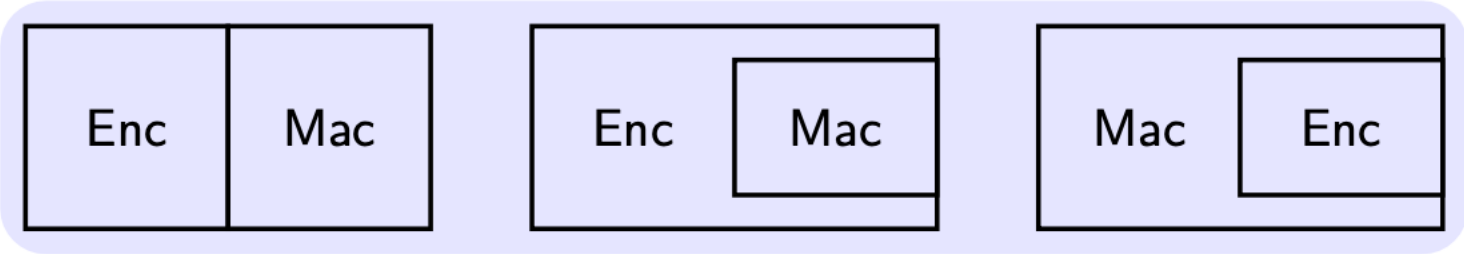
- 先定义保护真实性的认证通信，然后定义同时保护机密性和真实性的认证加密。
- 安全消息传递实验（**secure message transmission**） $\mathsf{Auth}_{\mathcal{A},\Pi'}(n)$:
  - $k = (k_1, k_2) \leftarrow \mathsf{Gen}'(1^n)$.
  - $\mathcal{A}$ 输入 1^n 和对 EncMac'_k的预言机访问，并输出 $c \leftarrow \mathsf{EncMac}'_k(m)$.
  - $m := \mathsf{Dec}'_k(c)$. $\mathsf{Auth}_{\mathcal{A},\Pi'}(n) = 1 \iff m \neq \perp \wedge m \notin \mathcal{Q}$.
- 定义：Π' 实现认证通信（**authenticated communication**），如果 $\forall$ ppt $\mathcal{A}$, $\exists$ negl 使得，$\Pr[\mathsf{Auth}_{\mathcal{A},\Pi'}(n) = 1] \leq \mathsf{negl}(n)$.
- 定义：Π' 是安全的认证加密（**secure Authenticated Encryption (A.E.)**）， 如果其既是CCA安全的也是实现了认证通信。
- 问题：CCA安全意味着A.E.吗？ （作业）

课堂练习

Suppose (E, D) provides A.E. Which of the following systems provide A.E.?

- $E'_k(m) = (E_k(m), E_k(m))$ and $D'_k(c_1, c_2) = D_k(c_1)$
- $E'_k(m) = (E_k(m), 0)$ and $D'_k(c, b) = \begin{cases} D_k(c) & \text{if } b = 0 \\ \perp & \text{otherwise} \end{cases}$
- $E'_k(m) = (E_k(m), E_k(m))$ and
  $D'_k(c_1, c_2) = \begin{cases} D_k(c_1) & \text{if } D_k(c_1) = D_k(c_2) \\ \perp & \text{otherwise} \end{cases}$
- $E'_k(m) = (E_k(m), H(m))$ (H is a CRHF) and
  $D'_k(c, h) = \begin{cases} D_k(c) & \text{if } H(D_k(c)) = h \\ \perp & \text{otherwise} \end{cases}$

加密和认证组合



- **Encrypt-and-MAC** (e.g., SSH (1995)):

$$c \leftarrow \mathsf{Enc}_{k_1}(m),\ t \leftarrow \mathsf{Mac}_{k_2}(m).$$

- **MAC-then-encrypt** (e.g, TLS 1.0 (1996), 802.11i WiFi (WPA2) (2004)):

$$t \leftarrow \mathsf{Mac}_{k_2}(m),\ c \leftarrow \mathsf{Enc}_{k_1}(m\|t).$$

- **Encrypt-then-MAC** (e.g, IPsec (1995), TLS $\geq$1.2 (2008)):

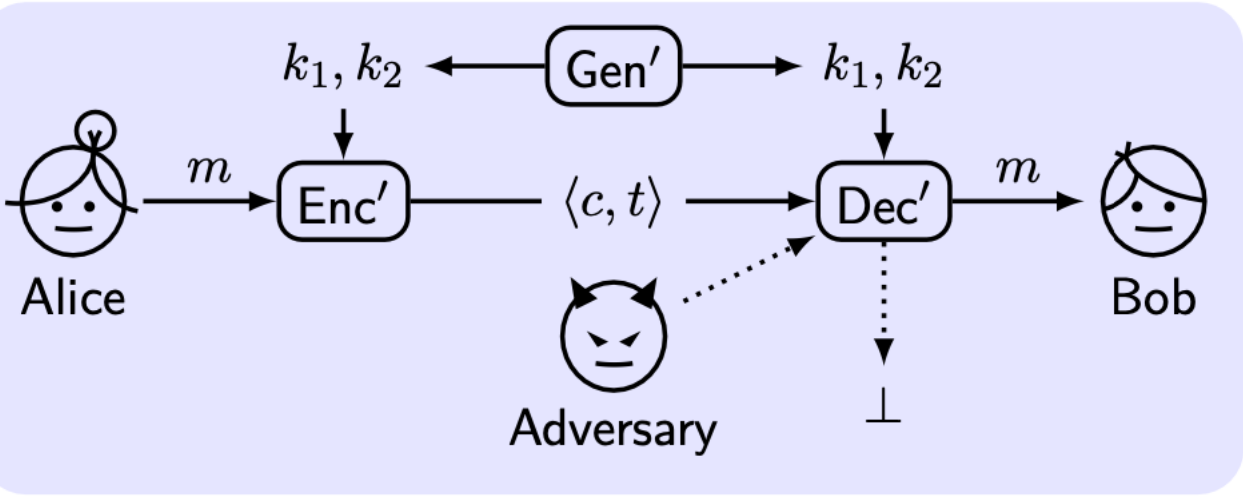
$$c \leftarrow \mathsf{Enc}_{k_1}(m),\ t \leftarrow \mathsf{Mac}_{k_2}(c).$$

分析组合安全性

- 采用全或无（All-or-nothing）分析，即一种组合方案要么在全部情况下都是安全的，要么只要存在一个不安全的反例就被认为是不安全的；
- 加密并认证: $\mathsf{Mac}'_k(m) = (m, \mathsf{Mac}_k(m))$.
  - 这表明，认证可能泄漏消息。
- 先认证后加密:
  - 一个例子：
    - $\mathsf{Trans}: 0 \to 00; 1 \to 10/01;$
    - Enc' 采用CTR模式; $c = \mathsf{Enc}'(\mathsf{Trans}(m \| \mathsf{Mac}(m)))$.
    - 将 c 的前两个比特翻转并且验证密文是否有效。$10/01 \to 01/10 \to 1$, $00 \to 11 \to \perp$.
      - 明文为1时，不改变明文；明文为0时，解密无效
    - 如果可以有效解密，则意味着消息的第一比特是1，否则是0；
    - 对于任何MAC，这都不是CCA安全的；
  - 这个例子表明，缺乏完整性保护时，敌手可解密，而密文是否有效也价值1个比特的信息。
- 先加密后认证: 解密: 如果 $\mathsf{Vrfy}(\cdot) = 1$， 那么 $\mathsf{Dec}(\cdot)$； 否则，输出 $\perp$。下面来证明。

AE安全方案

Idea: Make decryption oracle useless. AE(/CCA-secure) = CPA-then-MAC.



Construction 4

$\Pi_E = (\mathsf{Gen}_E, \mathsf{Enc}, \mathsf{Dec})$, $\Pi_M = (\mathsf{Gen}_M, \mathsf{Mac}, \mathsf{Vrfy})$. Π':

- $\mathsf{Gen}'(1^n)$: $k_1 \leftarrow \mathsf{Gen}_E(1^n)$ *and* $k_2 \leftarrow \mathsf{Gen}_M(1^n)$
- $\mathsf{Enc}'_{k_1,k_2}(m)$: $c \leftarrow \mathsf{Enc}_{k_1}(m)$, $t \leftarrow \mathsf{Mac}_{k_2}(c)$ *and output* $\langle c, t \rangle$
- $\mathsf{Dec}'_{k_1,k_2}(\langle c, t \rangle) = \mathsf{Dec}_{k_1}(c)$ *if* $\mathsf{Vrfy}_{k_2}(c, t) \stackrel{?}{=} 1$; *otherwise* $\perp$

AE理论与实践

- 定理：\Pi_E 是CPA安全的并且 \Pi_M 是一个带有唯一标签的安全MAC（强安全MAC），那么由先加密后认证得到的 \Pi' 是安全的。
  注：强安全MAC是指一个消息只有一个有效标签
  - GCM (Galois/Counter Mode): 先CTR加密，然后做 Galois MAC. (RFC4106/4543/5647/5288 on IPsec/SSH/TLS)
  - EAX: 先CTR 加密，然后 CMAC（Cipher-based MAC）。
- 定理：先认证后加密方法是安全的，如果 \Pi_E 是CTR模式或者CBC模式。
  - CCM (Counter with CBC-MAC): 先 CBC-MAC 后 CTR 加密。(802.11i, RFC3610)
  - OCB (Offset Codebook Mode): 将MAC整合到加密中。（是CCM, EAX的2倍快）
- 上述方案都支持 AEAD (A.E. with associated data): 部分是明文并且整个消息被认证。这在实践中是很常用的，例如一个IP报文需要加密，但IP头部需要以明文方式传输。

实现漏洞

- 实现可能摧毁理论上的安全性：
  - Padding Oracle 攻击（TLS 1.0）：解密返回两种类型错误: padding error，MAC error；敌手通过猜测来获得最后一字节，如果没有padding错误；参考之前在CCA部分学习的Padding Oracle攻击；
  - 攻击非原子解密（SSH Binary Packet Protocol）：解密时，分三步 (1)解密消息长度；(2)读取长度所表明的包数；(3) 检查MAC；敌手针对这种非原子解密过程，实施攻击分三步 (1)发送密文 c；(2)发送 l 个包直到“MAC error”发生；(3)获得密文对应的明文 l = \mathsf{Dec}(c)。

本节小结

- 先加密后认证得到A.E.（包含CCA）