应用密码学研究生课程

Kurt Pan

2023 年 5 月 26 日

目录

目录

第 1 章

公钥工具

我们首先通过介绍几个基本工具来开始讨论公钥密码学，这些工具将在本书的其余部分中使用。这些工具的主要应用将在接下来的几章中出现，我们将在那里使用它们进行公钥加密、数字签名和密钥交换。由于我们在本章中使用了一些基本的代数和数论，因此建议读者首先简单地浏览一下附录 A。

我们从一个简单的玩具问题开始：在两方之间生成一个共享的秘密密钥，以便被动窃听敌手不能猜测出他们的共享密钥。敌手可以监听网络流量，但不能修改在途的消息或注入他自己的消息。在后面的章节中，我们开发了在存在可能干扰网络流量的主动攻击者的情况下进行密钥交换所需的全部设备。

我们在开始时就强调，对窃听的安全性通常不足以应对真实世界的应用，因为有能力监听网络流量的攻击者通常也能够篡改它；然而，这个玩具窃听模型是介绍新公钥工具的好方法。

1.1 玩具问题：匿名密钥交换

1.2 单向陷门函数

In this section, we introduce a tool that will allow us to build an efficient and secure key exchange protocol. In Section 8.11, we introduced the notion of a one-way function. This is a function $F : \mathcal{X} \to \mathcal{Y}$ that is easy to compute, but hard to invert. As we saw in Section 8.11, there are a number of very efficient functions that are plausibly one-way. One-way functions, however, are not sufficient for our purposes. We need one-way functions with a special feature, called a trapdoor. A trapdoor is a secret that allows one to efficiently invert the function; however, without knowledge of the trapdoor, the function remains hard to invert. Let us make this notion more precise.

本节将介绍一个工具，让我们能够构造高效且安全的密钥交换协议。在 8.11 节中，我们介绍了单向函数的概念。这是一个易于计算但难以求逆的函数 $F : \mathcal{X} \to \mathcal{Y}$。正如我们在 8.11 节中看到的，有许

多非常高效的函数似乎是单向的。然而，单向函数不足以满足我们的目的。我们需要具有特殊功能的单向函数，称为陷门。陷门是一个秘密，可以让人们有效地反转功能；然而，在不知道暗门的情况下，该函数仍然难以反转。

让我们使这个概念更精确。

定义 1.1 (陷门函数方案)**.** 令 $\mathcal{X}$ 和 $\mathcal{Y}$ 为有限集合。一个定义在 $(\mathcal{X}, \mathcal{Y})$ 上的陷门函数方案 $\mathcal{T}$ 包括三部分的算法 (G, F, I)，其中

- G 是概率性的密钥生成算法，调用方式如下：$(pk, sk) \xleftarrow{R} G()$，其中 pk 称为公钥，sk 称为私钥。
- F 是确定性的算法，调用方式如下：$y \leftarrow F(pk, x)$，其中 pk 是公钥（由 G 输出），x 在 $\mathcal{X}$ 中。输出 y 是 $\mathcal{Y}$ 的一个元素。
- I 是确定性的算法，调用方式如下：$x \leftarrow I(sk, y)$，其中 sk 是一个私钥（由 G 输出）且 y 在 $\mathcal{Y}$ 中。输出 x 是 $\mathcal{X}$ 的一个元素。

此外，应满足以下正确性性质：对于 $G()$ 的所有可能输出（ pk, sk），以及对于所有 $x \in \mathcal{X}$，我们有 $I(sk, F(pk, x)) = x$。

定理 1.1. *test*

定义 1.2. We say that a trapdoor function scheme $\mathcal{T}$ is one way if for all efficient adversaries $\mathcal{A}$, the quantity $\mathsf{OWadv}[\mathcal{A}, \mathcal{T}]$ is negligible.

Note that in Attack Game 10.2, since the value x is uniformly distributed over $\mathcal{X}$ and $F(pk, \cdot)$ is one-to-one, it follows that the value $y := F(pk, x)$ is uniformly distributed over the image of $F(pk, \cdot)$. In the case of a trapdoor permutation scheme, where $\mathcal{X} = \mathcal{Y}$, the value of y is uniformly distributed over $\mathcal{X}$.

1.2.1 使用单向陷门函数方案的密钥交换

1.2.2 数学细节

As usual, in defining the one-wayness security property, we parameterize Attack Game 10.2 by the security parameter λ, and the advantage $\mathrm{OWadv}[\mathcal{A}, \mathcal{T}]$ is actually a function of λ. Definition 10.3 should be read as saying that $\mathrm{OWadv}[\mathcal{A}, \mathcal{T}](\lambda)$ is a negligible function.

参考文献

[ALM+98] Sanjeev Arora et al. *Proof verification and the hardness of approximation problems*. Journal of the ACM (JACM) 45.3 (1998), pp. 501–555.

[AS98] Sanjeev Arora and Shmuel Safra. *Probabilistic checking of proofs: A new characterization of NP*. Journal of the ACM (JACM) 45.1 (1998), pp. 70–122.

[BFL91] László Babai, Lance Fortnow, and Carsten Lund. *Non-deterministic exponential time has two-prover interactive protocols*. Computational complexity 1 (1991), pp. 3–40.

[LFK+92] Carsten Lund et al. *Algebraic methods for interactive proof systems*. Journal of the ACM (JACM) 39.4 (1992), pp. 859–868.

[Sch89] Claus-Peter Schnorr. *Efficient Identification and Signatures for Smart Cards*. Annual International Cryptology Conference. 1989.

[Sha92] Adi Shamir. *IP = PSPACE*. Journal of the ACM (JACM) 39.4 (1992), pp. 869–877.

参考文献