第七讲：通信安全协议及应用

一、协议的基本概念

二、零知识证明技术

三、Coin-Flipping by Phone

一、协议的基本概念

协议 (Protocol)，就是两个或两个以上的参与者为完成某项特定的任务而采取的一系列步骤。这个定义包含三层含义：

- 第一，协议自始至终是有序的过程，每一步骤必须依次执行。在前一步没有执行完之前，后面的步骤不可能执行；
- 第二，协议至少需要两个参与者。一个人可以通过执行一系列的步骤来完成某项任务，但它不构成协议；
- 第三，通过执行协议必须能够完成某项任务。即使某些东西看似协议，但没有完成任何任务，也不能成为协议，只不过是浪费时间的空操作。

一、协议的基本概念

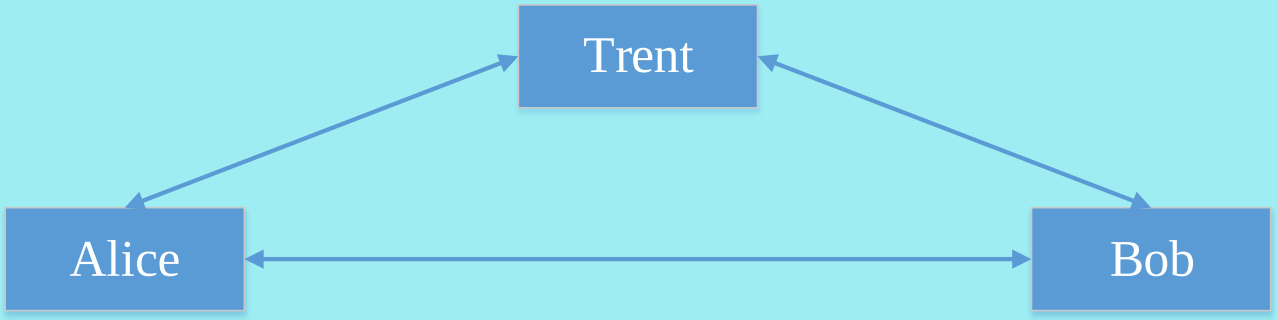
协议的参与者及其在协议中所发挥的作用：

Alice	在所有协议中，她是第一参与者
Bob	在所有的协议中，他是第二参与者
Carol	在三方或四方协议中，他是参与者之一
David	在三方或四方协议中，他是参与者之一
Eve	窃听者
Mallory	恶意的主动攻击者
Trent	可信赖的仲裁者
Peggy	证明者
Victor	验证者
Walter Warden	他将在某些协议中保护 Alice 和 Bob

一、协议的基本概念

1. 仲裁协议

仲裁者 (Arbitrator) 是某个公正的第三方。在执行协议的过程中，其它各方均信赖他。“**公正**”意味着仲裁者对参与协议的任何一方没有偏向，而“可信赖”意味着参与协议的所有人均认为他所说的话都是真的，他所做的事都是正确的，并且他将完成协议赋予他的任务。仲裁者能够帮助两个互不信赖的实体完成协议。



(*a*) 仲裁协议

一、协议的基本概念

例：Alice和Bob买卖车可以通过执行以下协议来确保彼此不受欺骗：

① Alice将车主权和钥匙交给律师。

② Bob将支票交给Alice。

③ Alice在银行兑现支票。

④ 在规定的时间内，若证明支票是真的，律师将车主权和钥匙交给Bob；若证明支票是假的，Alice将向律师提供确切的证据，此后律师将车主权和钥匙交还给Alice。

在这一协议中，Alice相信在他弄清支票的真伪之前，律师不会将车主权交给Bob。一旦发现支票有假，律师还会将车主权归还他；Bob也相信律师在支票兑现后，将把车主权和钥匙交给他。在协议中，律师只起担保代理作用，他并不关心支票的真伪。

一、协议的基本概念

例：银行也可以充当仲裁人的角色。通过执行以下协议，Bob可以从 Alice 手中买到车：

① Bob 开一张支票并将其交给银行。

② 在验明 Bob 的钱足以支付支票上的数目后，银行将保付支票交给Bob。

③ Alice 将车主权和钥匙交给 Bob。

④ Bob 将保付支票交给 Alice。

⑤ Alice 兑现支票。

这个协议是有效的，因为 Alice 相信银行的开具的证明。同时，他也相信银行不会将他的钱用于其它不正当的场合。

一、协议的基本概念

2. 裁决协议 (Adjudicated Protocol) 。在协议中引入仲裁人会增加系统的造价，所以在实际中，我们引入另外一种协议，称为**裁决协议**。只有发生纠纷时，裁决人才执行此协议；而无纠纷发生时，并不需要裁决人的参与。

裁决人 (Adjudicator) 也是一个公正的、可信赖的第三方。他不像仲裁者一样直接参与协议。例如，法官是职业裁决人。Alice 和 Bob 在签署合同时，并不需要法官的参与。但是，当他们之间发生纠纷时，就需要法官来裁决。

一、协议的基本概念

合同签署协议可如下表述：

无仲裁的子协议：

(1) Alice 和 Bob 协商协议的条款。

(2) Alice 签署这个合同。

(3) Bob 签署这个合同。

裁决子协议：

(4) Alice 和 Bob 出现在法官面前。

(5) Alice 向法官提供她的证据。

(6) Bob 向法官提供他的证据。

(7) 法官根据双方提供的证据进行裁决。

一、协议的基本概念

在计算机网络环境下，也有裁决协议。这些协议建立在各方均是诚实的基础之上。但是，当有人怀疑发生欺骗时，可信赖的第三方就可以根据所存在的某个数据项判定是否存在欺骗。一个好的裁决协议应该能够确定欺骗者的身份。注意，裁决协议只能检测欺骗是否存在，而不能防止欺骗的发生。

3. 自动执行协议 (Self-Enforcing Protocol)

自动执行协议是最好的协议。协议本身就保证了公平性这种协议不需要仲裁者的参与，也不需要裁决者来解决争端。如果协议中的一方试图欺骗另一方，那么另一方会立刻检测到该欺骗的发生，并停止执行协议。

一、协议的基本概念

好的协议应该具有以下特点：

- 协议涉及的每一方必须事先知道此协议以及要执行的所有步骤。
- 协议涉及的每一方必须同意遵守协议。
- 协议必须是非模糊的。对协议的每一步都必须确切定义，力求做到避免产生误解。
- 协议必须是完整的。对每一种可能发生的情况都要作出反应。
- 每一步操作要么是由一方或多方进行计算，要么是在各方之间进行消息传递，二者必居其一。

一、协议的基本概念

许多面对面的协议依赖于人出场来保证真实性和安全性。例如，你购物时，不可能将支票交给陌生人；你与他人玩扑克时，必须保证亲眼看到他洗牌和发牌。然而，当你通过计算机与远端的用户进行交流时，真实性和安全性便无法保证。实际上，我们不仅难以保证使用计算机网络的所有用户都是诚实的，而且也难以保证计算机网络的管理者和设计者都是诚实的。只有通过使用规范化协议，才可以有效地防止不诚实的用户对网络实施的各种攻击。

从上面的讨论可知，计算机网络中使用的好的通信协议，不仅应该具有**有效性**、**公平性**和**完整性**，而且应该具有足够高的**安全性**。通常我们把具有安全性功能的协议称为安全协议。安全协议的设计必须采用密码技术。因此，我们有时也将安全协议称作密码协议。

一、协议的基本概念

密码协议与许多通信协议的显著区别在于它使用了密码技术。在进行密码协议的设计时，常常要用到某些密码算法。密码协议所涉及的各方可能是相互信赖的，也可能彼此互不信任。当成千上万的用户在网络上进行信息交互时，会给网络带来严重的安全问题。例如，非法用户不必对网络上传输的信息解密，就可能利用网络协议自身存在的安全缺陷，获取合法用户的某些机密信息（如用户口令、密钥、用户身份号等），从而冒充合法用户无偿使用网络资源，或窃取网络数据库中的秘密用户文档。因此，设计安全、有效的通信协议，是密码学和通信领域中一个十分重要的研究课题。密码协议的目标不仅仅是实现信息的加密传输，而更重要的是为了解决通信网的安全问题。参与通信协议的各方可能想分享部分秘密来计算某个值、生成某个随机序列、向对方表明自己的身份，或签订某个合同。在协议中采用密码技术，是防止或检测非法用户对网络进行窃听和欺骗攻击的关键技术措施。所谓协议是安全的，意味着非法用户不可能从协议中获得比协议自身所体现的更多的、有用的信息。

二、零知识证明技术

1. 概述

示证者：P；

验证者：V；

最大泄露证明：出示或说出此事物，使别人相信，但同时使别人也知道或掌握了这一秘密；

最小泄露证明和零知识证明：以一种有效的数学方法，使V可以检验每一步成立，最终确信P知道其秘密，而又能保证不泄露P所知道的信息。

二、零知识证明技术

最小泄露证明满足下述条件：

① 示证者几乎不可能欺骗验证者，若 P 知道证明，则可使 V 几乎确信 P 知道证明；若 P 不知道证明，则他使 V 相信他知道证明的概率近于零。

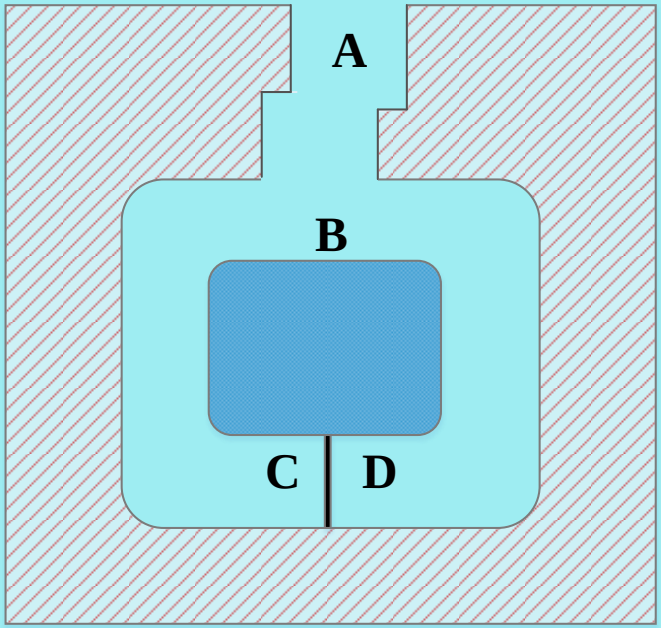
② 验证者几乎不可能得到证明的信息，特别是他不可能向其他人出示此证明。

③ 验证者从示证者那里得不到任何有关证明的知识。

交互作用协议： V 向 P 提问，若 P 知道证明则可正确回答 V 的提问；若 P 不知道证明，则对提问给出正确回答概率仅为1/2。V 以足够多的提问就可推定 P 是否知道证明，且要保证这些提问及其相应的回答不会泄露出有关 P 所知道的知识。

二、零知识证明技术

2. 零知识证明的基本协议：[Quisquater 等1989]



设 P 知道咒语，可打开 C 和 D 之间的秘密门，不知道者都将走向死胡同中。

图1 零知识证明概念图解

二、零知识证明技术

协议 1:

① V 站在 A 点;

② P 进入洞中任一点 C 或 D;

③ 当 P 进洞之后，V 走到 B 点;

④ V 叫 P：(a)从左边出来，或(b)从右边出来;

⑤ P 按要求实现(以咒语，即解数学难题帮助);

⑥ P 和 V 重复执行①～⑤共n次。

若 A 不知咒语，则在 B 点，只有50%的机会猜中 B 的要求，协议执行n次，则只有2^{-n}的机会完全猜中，若n =16，则若每次均通过 B 的检验，B 受骗机会仅为1/65 536。

二、零知识证明技术

此协议又称作**分割和选择** (Cut and Choose) 协议，是公平分享东西时的经典协议。即**协议 2：**

① A 将东西切成两半；

② B 选其中之一；

③ A 拿剩下的一半。

显然，A为了自己的利益在 (1) 中要公平分割，否则(2) 中 B 先于他的的选择将对其不利。Rabin [1978] 最早将此用于密码学，后来发展为交互作用协议和零知识证明[Golrreich 等 1985 , 1989]。此洞穴问题可以换成数学问题，A知道解决某个难题的秘密信息，而B通过与A交互作用验证其真伪。

二、零知识证明技术

协议 3：

① A 用其信息和某种随机数将难题转成另一种难题，且与原来的同构，A 可用其信息和随机数解新的难题；

② A 想出新的难题的解，采用 Bit 承诺方案；

③ A 将新难题出示给 B，但 B 不能由此新难题得到有关原问题或其解；

④ B 向 A 提下述问题之一：(a) 向 B 证明老和新问题是同构的，(b) 公开(2)中的解，并证明它是新难题的解；

⑤ A 按 B 的要求执行；

⑥ A 和 B 重复执行 ①～⑤ 共 n 次。

必须仔细选择适当问题和随机信息，使 B 即使重复执行多次协议也得不到有关原问题的任何信息。并非所有的“难题”都可用于零知识证明，但有不少可用于此。

二、零知识证明技术

3. 并行零知识证明: 执行 n 次协议可以并行方式实施。

协议4:

① A 用其信息及某种随机数将难题变换成 n 个不同的同构问题，而后用其信息和随机数解 n 个新的难题;

② A 完成 n 个新的难题的解;

③ A 向 B 披露 n 个新的难题，而 B 不能从中得到原问题或其解的信息;

④ B 向 A 提出有关 n 个新的难题的提问：(a) 出示新旧难题的同构性证明，或(b)公布②中新的难题的解，并证明是新难题的解;

⑤ A 回答提问。

二、零知识证明技术

4. 使第三者相信的协议 (零知识)

B 若想使 C 相信 A 知道某信息，他将与 A 执行协议的复本给 C 能否使 C 相信？否，因为两个不知秘密信息的人可以串通一起来骗 C。例如，诈骗者 A 可以假装知道秘密，并与 B 串通，让 B 只提出 A 可以答对的问题，这样得到的 A 与 B 执行协议的复本就可能骗 C。

5. 非交互式零知识证明

上述二中的协议都是交互式的，难以C相信A与B没有勾结。若要使 C 和其他人相信，应采用**非交互式** (Non interactive) 零知识证明。对于非交互式零知识证明， A 可以公布证明，任何人可以花时间检验该证明的正确性。

二、零知识证明技术

6. 一般化理论结果

- Blum 证明：任何数学问题可化为图论中问题，其证明等价于 Hamiltonian 回路问题，由此可以构成零知识证明问题，任何掌握这一数学问题的人都可以利用零知识证明来公布这一结果，使别人相信而不泄露证明方法。
- Burmester 等提出广播交互式证明问题。
- 一些密码学家证明可以用交互证明的问题都可以化为零知识交互证明的问题。可由此给出各种变型、协议及应用。

三、 Coin-Flipping by Phone

Alice and Bob want to decide whether to go to the Cinema or the Opera in a fair way.

1、使用单向函数的投币协议

① Alice 随机选择一个数 x， 计算 $y = f(x)$ 。

② Alice 把 y 送给 Bob。

③ Bob 猜测 x 是奇数还是偶数，将猜测结果发给 Alice。

④ Alice 发送 x 给 Bob， Bob 验证自己是否猜对。

⑤ 如果 x 是偶数，那么表示结果为正面，去 Cinema；否则，为反面，去 Opera.

三、 Coin-Flipping by Phone

分析：

1. 如果两方都诚实，那么该协议有效。安全性基于 f 的单向性。
2. Alice 能欺骗 Bob 吗？她是否有一个有利的条件？ x 的随机性怎么保证？
3. 如何修改使得 Alice 没有有利的条件？利用选择-分割协议，如果 Bob 猜对就为反面，猜错为正面。

三、 Coin-Flipping by Phone

2、使用公钥技术的投币协议

① Alice 随机选择两个消息 m_1, m_2，利用自己的公钥加密得到 $E_A(m_1), E_A(m_2)$送给Bob.

② Bob 随机选择一个利用自己的公钥加密得到 $E_B(E_A(m))$送给 Alice

③ Alice 用自己的私钥解密$D_A(E_B(E_A(m)))$ 得到$E_B(m)$ 发给Bob。

④ Bob 解密得到 m 。

⑤ 如果$m = m_1$，那么表示结果为正面，去Cinema；否则，为反面，去 Opera.

⑥ Alice 和 Bob 分别公布自己的私钥，让对方验证自己没有欺骗

thank you