实体认证
Authentication

协议的定义

协议是两个或更多的参与者为完成某项特定的任务而采取的一系列步骤。

1. 协议自始至终是有序的过程，每一步骤必须依次执行，在前一步骤没有执行完之前，后面的步骤不能执行。

2. 协议至少需要两个参与者。

3. 通过执行协议必须能够完成某项任务。

实体认证协议

协议是两个或更多的参与者为完成某项特定的任务而采取的一系列步骤。

一般是2-3个参与者为完成1-2个参与者的身份认证任务而采取的1-5个步骤。

协议与算法的区别

实体认证协议 VS 数字签名算法/消息认证码算法

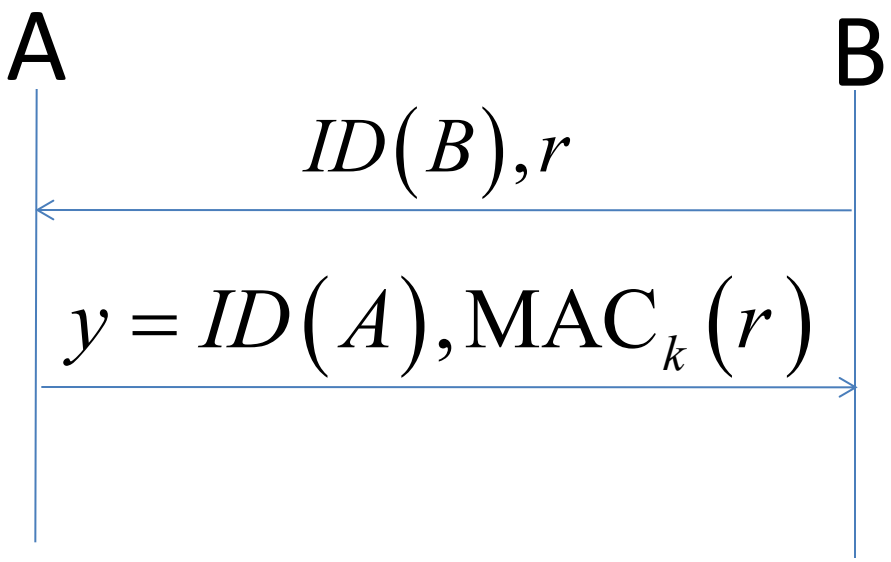
实体认证协议的目标是确认实体身份，对确认时间范围有规定。

数字签名算法/消息认证码算法的目标是确认消息源，且对确认时间范围没有规定。

实体认证协议实例

一个直觉上的实体认证协议

(2个参与者为完成1个参与者的身份认证任务而采取的2个步骤)



1) Bob选择一个随机挑战 r 发送给Alice $ID(B), r$

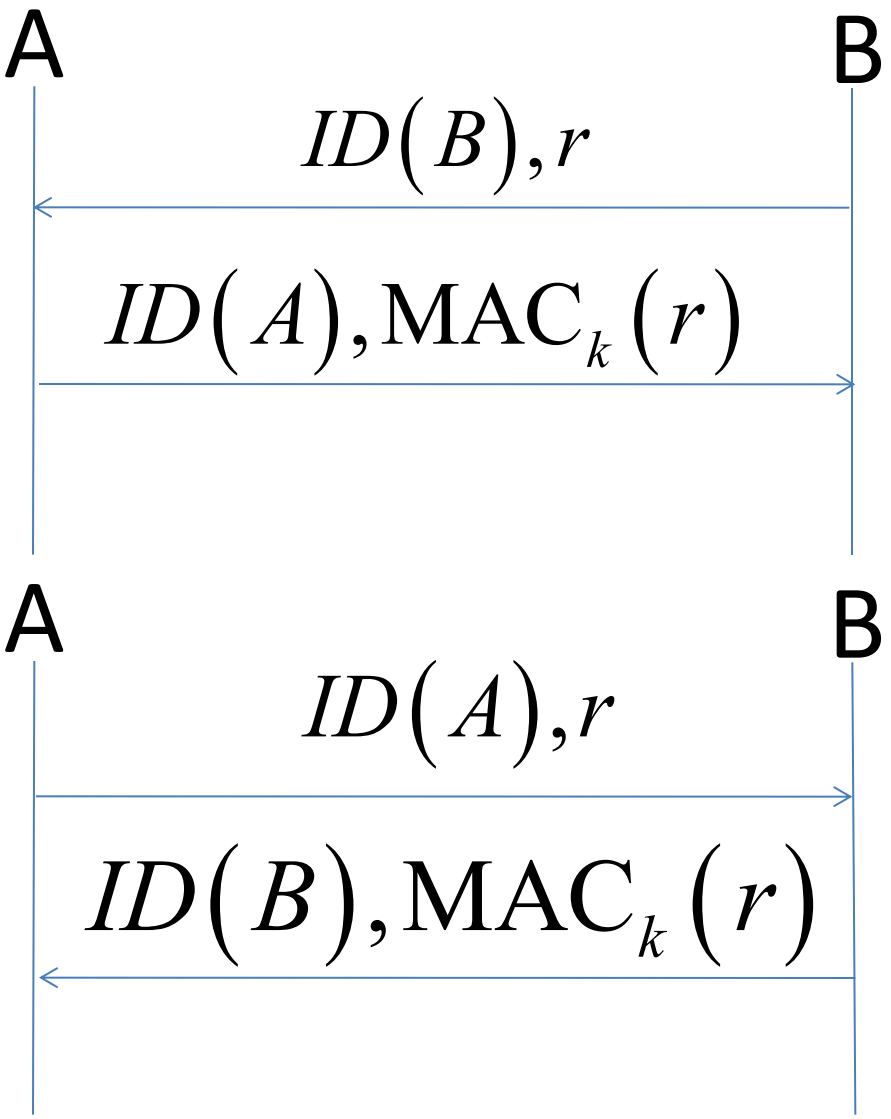
2) Alice计算 y 发送给Bob

3) Bob计算 $y' = \mathrm{MAC}_k(r)$ 如果 $y = ID(A) \| y'$, Bob接受，否则Bob拒绝

实体认证协议攻击实例

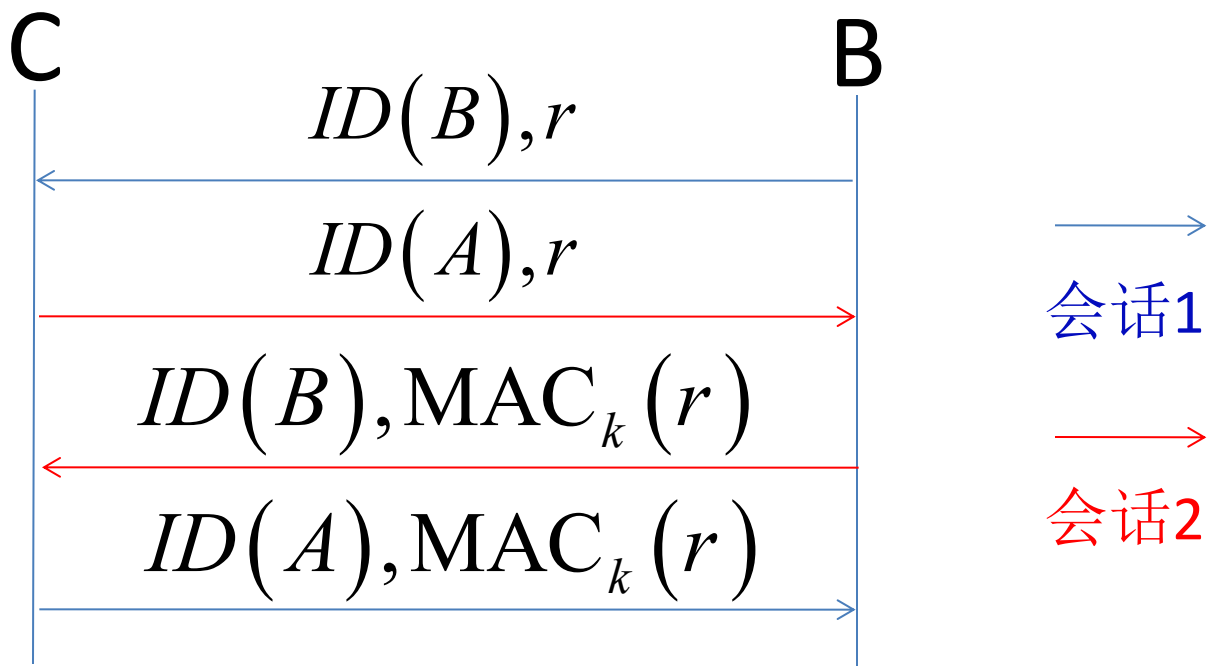
不安全在哪？

如何攻击？



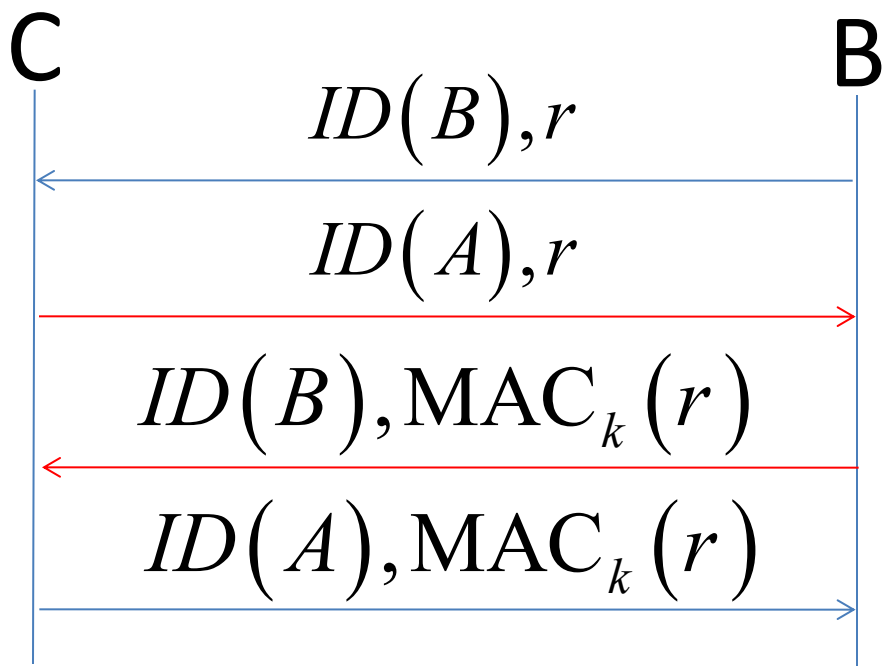
实体认证协议攻击实例

即使消息认证码算法是安全的，前页的实体认证协议也是不安全的，如C可以冒充A与B按如下步骤执行。



实体认证协议攻击实例

即使消息认证码算法是安全的，前页的实体认证协议也是不安全的，如C可以冒充A与B按如下步骤执行。



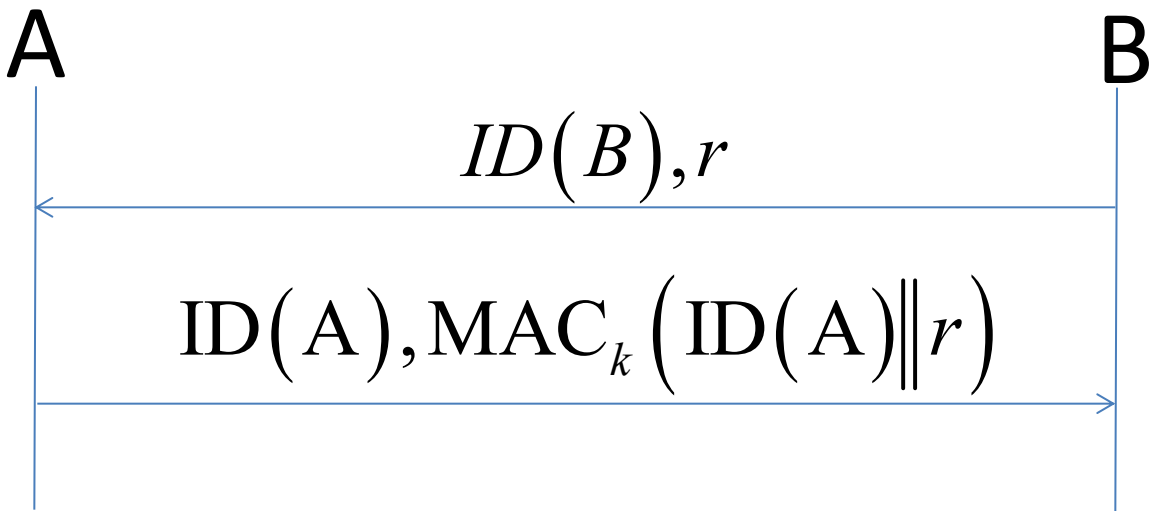
1. 协议自始至终是有序的过程，每一步骤必须依次执行，在前一步骤没有执行完之前，后面的步骤不能执行。

2. 协议至少需要两个参与者。

3. 通过执行协议必须能完成某项任务。

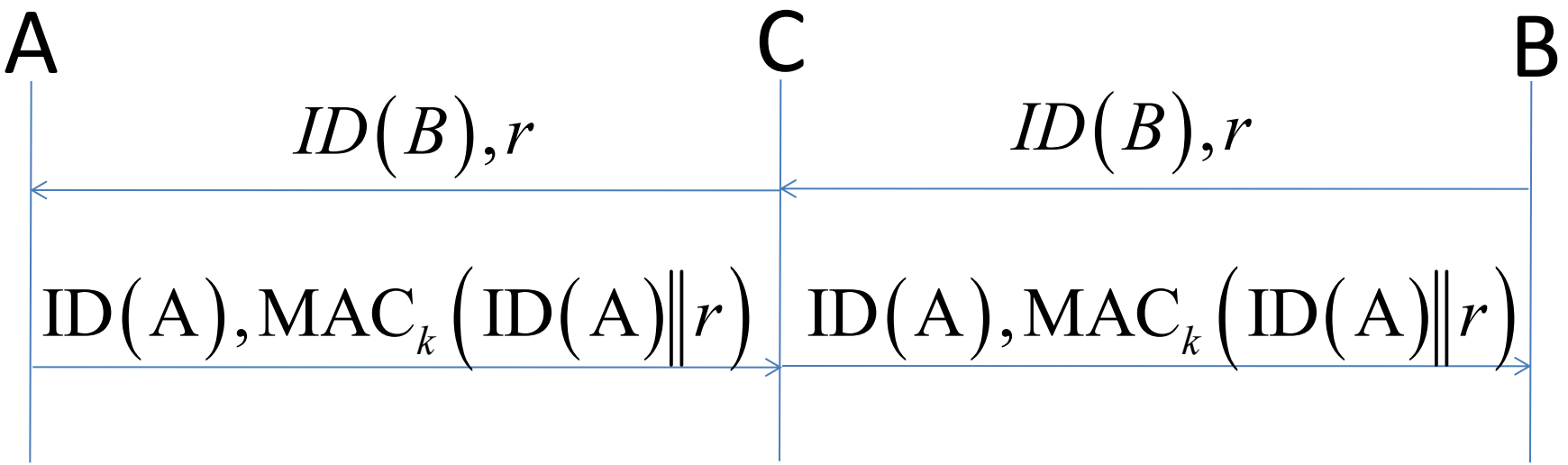
实体认证协议实例

改进的实体认证协议



协议攻击

对上页实体认证协议的一种“攻击”



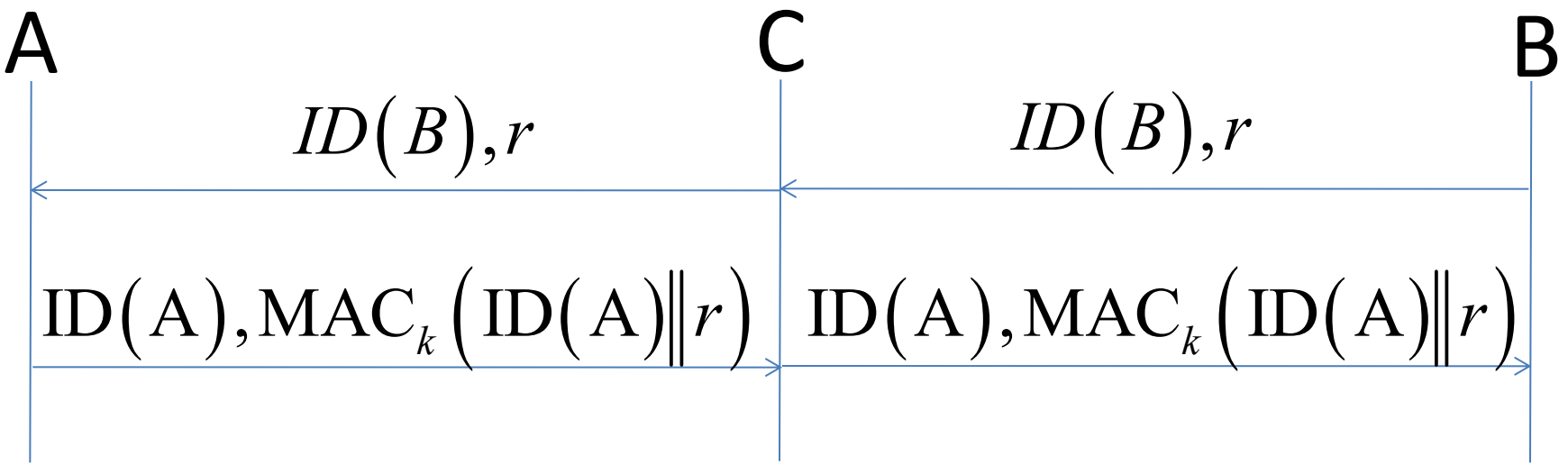
1. 协议自始至终是有序的过程，每一步骤必须依次执行，在前一步骤没有执行完之前，后面的步骤不能执行。

2. 协议至少需要两个参与者。

3. 通过执行协议必须能完成某项任务。

协议攻击

对上页实体认证协议的一种“攻击”



这不算是攻击，因为敌手C只进行了存储和转发。

C可视为一个路由器。

协议攻击的判定

对协议攻击的判定方法：

1. 协议中的任意一个或多个参与者并未依次执行协议。
2. 执行协议后并未完成任务。

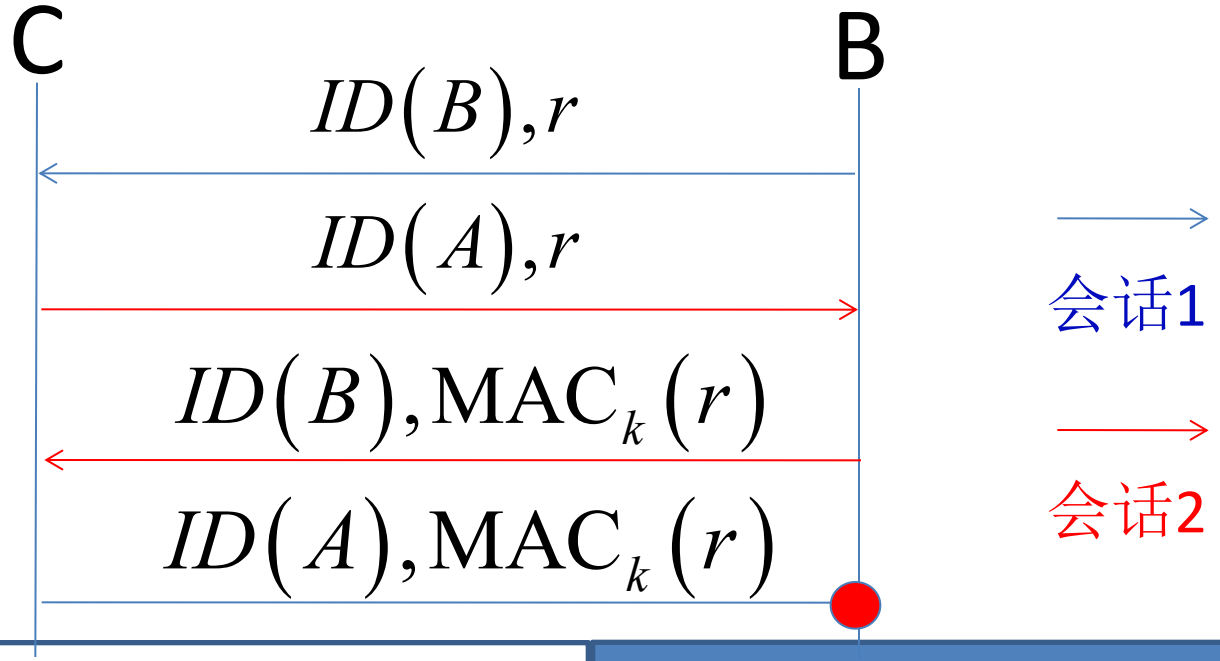
满足以上两条中的任意一条即可视为攻击。

协议攻击的判定

对协议攻击的判定方法：

1. 协议中的任意一个或多个参与者并未依次执行协议。
2. 执行协议后并未完成任务。

这是对身份认证协议的攻击吗？

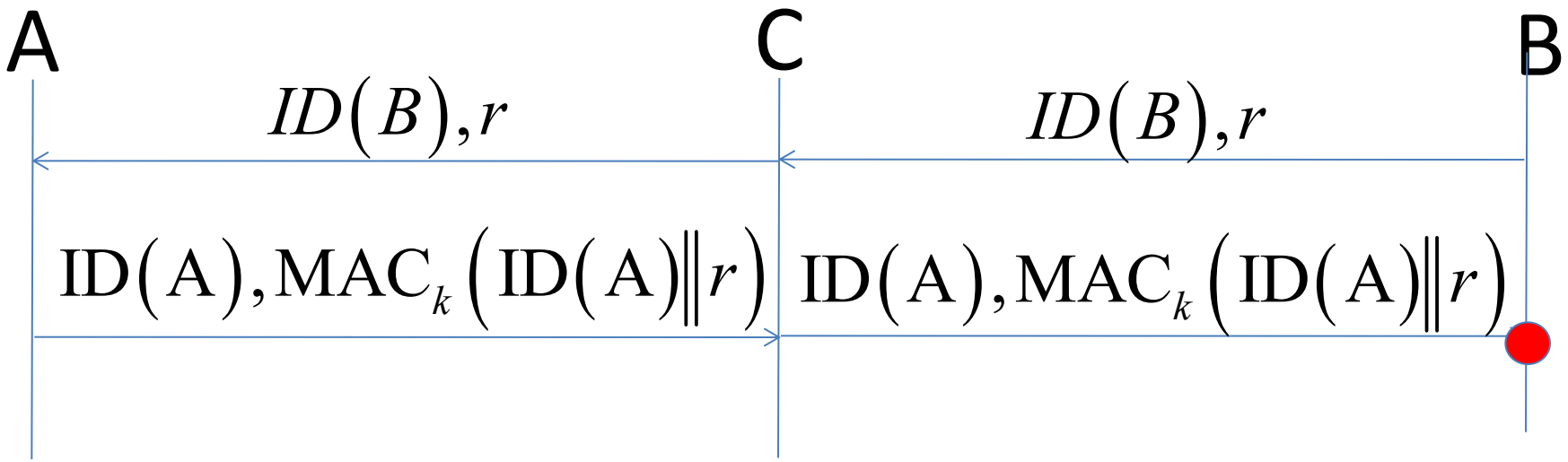


协议攻击的判定

对协议攻击的判定方法：

1. 协议中的任意一个或多个参与者并未依次执行协议。
2. 执行协议后并未完成任务。

这是对身份认证协议的攻击吗？



密码协议的安全性分析

安全性的证明整体思路：

1. 定义什么是安全。（这等价于定义了什么是不安全）

2. 假定协议中用到的密码算法是满足第一步的定义的。

   对称/非对称加密算法、Hash算法、MAC算法、签名算法等

3. 证明如果存在一个敌手可以攻破协议，那么利用这个敌手就可以攻破对应的密码算法。

实体认证协议的安全性分析

以前页实体协议为例：

1. 定义安全：敌手在运行$q(n)$次协议/算法后，攻陷协议/算法的概率$\varepsilon(n)$可以忽略

2.假定协议中用到的MAC算法是安全的，换句话说，查询$q(n)$个值对应的MAC值后，敌手成功伪造出一个有效的消息验证码的概率不超过$\varepsilon(n)$

3.证明：如果协议不安全，那么MAC算法一定也不安全。

实体认证协议的安全性分析

运行$q(n)$次协议，等价于敌手知道了$q(n)$个 $\mathrm{ID}(\mathrm{A})\|r$ 对应的

MAC值，$\mathrm{MAC}_k\left(\mathrm{ID}(\mathrm{A})\|r\right)$

此时，对于一个随机挑战r'，可以伪造出第二条消息的概率

$$
\begin{aligned}
&\Pr[\mathrm{Success}] \\
&= \Pr[\mathrm{Query}]\Pr[\mathrm{Success} \mid \mathrm{Query}] \\
&+ \Pr[\overline{\mathrm{Query}}]\Pr[\mathrm{Success} \mid \overline{\mathrm{Query}}] \\
&\le \Pr[\mathrm{Query}] + \Pr[\mathrm{Success} \mid \overline{\mathrm{Query}}]
\end{aligned}
$$

Query表示随机挑战r'在$q(n)$次协议的运行中曾经出现过，也就是说敌手知道r'对应的MAC值

实体认证协议的安全性分析

$$
\begin{aligned}
&\Pr[\text{Success}] \\
&= \Pr[\text{Query}]\Pr[\text{Success} \mid \text{Query}] \\
&+ \Pr[\overline{\text{Query}}]\Pr[\text{Success} \mid \overline{\text{Query}}] \\
&\le \Pr[\text{Query}] + \Pr[\text{Success} \mid \overline{\text{Query}}]
\end{aligned}
$$

Query表示随机挑战r'在$q(n)$次协议的运行中曾经出现过，也就是说敌手知道r'对应的MAC值

显然，$\Pr[\text{Query}] \le \dfrac{q(n)}{2^n}$ ，因此可忽略。

$\overline{\text{Query}}$表示 r' 与$q(n)$个 r 均不相同，此时如果敌手成功伪造出协议的第二条消息等价于成功伪造出了 $\text{MAC}_k\left(\text{ID}(\text{A})\|r'\right)$

实体认证

主动攻击

1. 敌手产生了一个消息，并放入信道。

2. 敌手改变信道中的消息。

3. 敌手转移信道中的消息，发送给其他人，而不是指定接受者。

满足上述三条中的任何一条就说敌手进行了主动攻击。

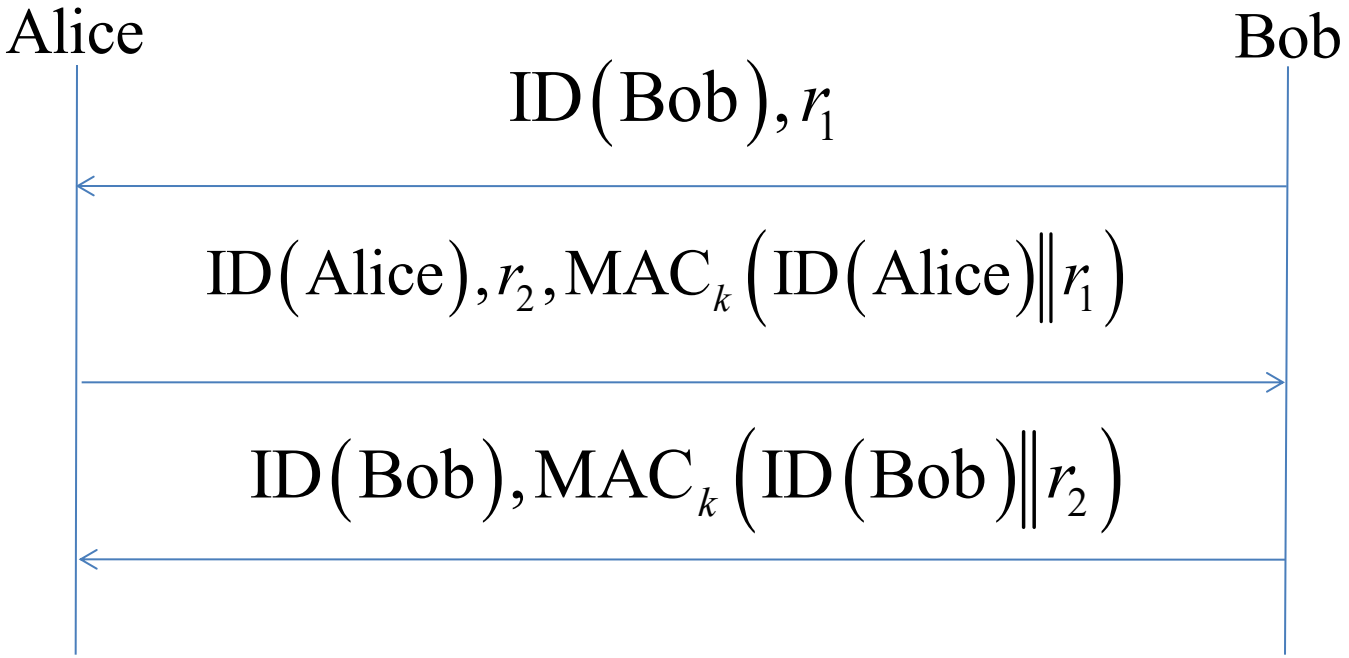
实体认证

交互认证（双向认证）

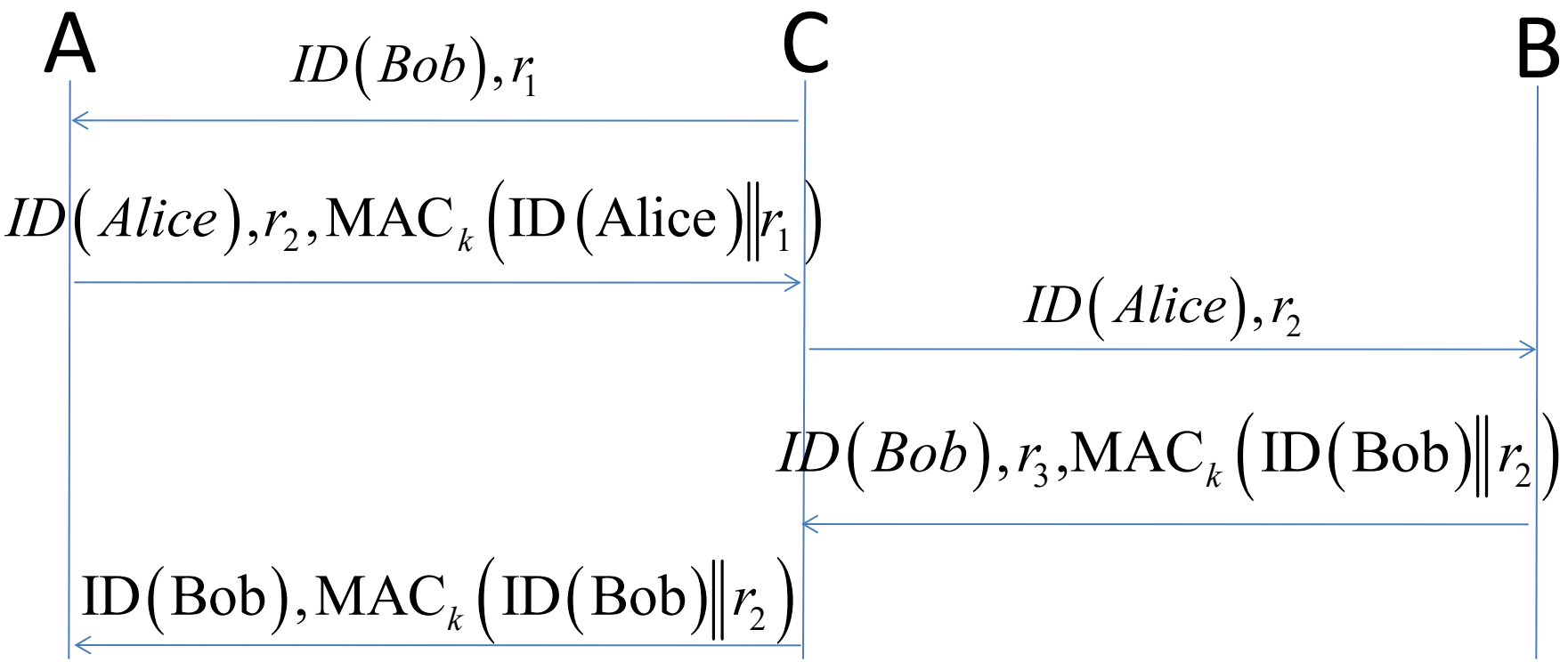
交互认证也称为交互身份识别。会话成功完成时，参与双方都为“接受”状态。敌手试图欺骗Alice或Bob或双方，使其接受。敌手的目标是进行主动攻击后，使得诚实的参与方“接受”。显然可以运行两次安全的挑战-响应方案实现双向认证，但是我们希望同时将其合并为一个方案。

双向实体认证协议实例

直觉上的双向认证协议

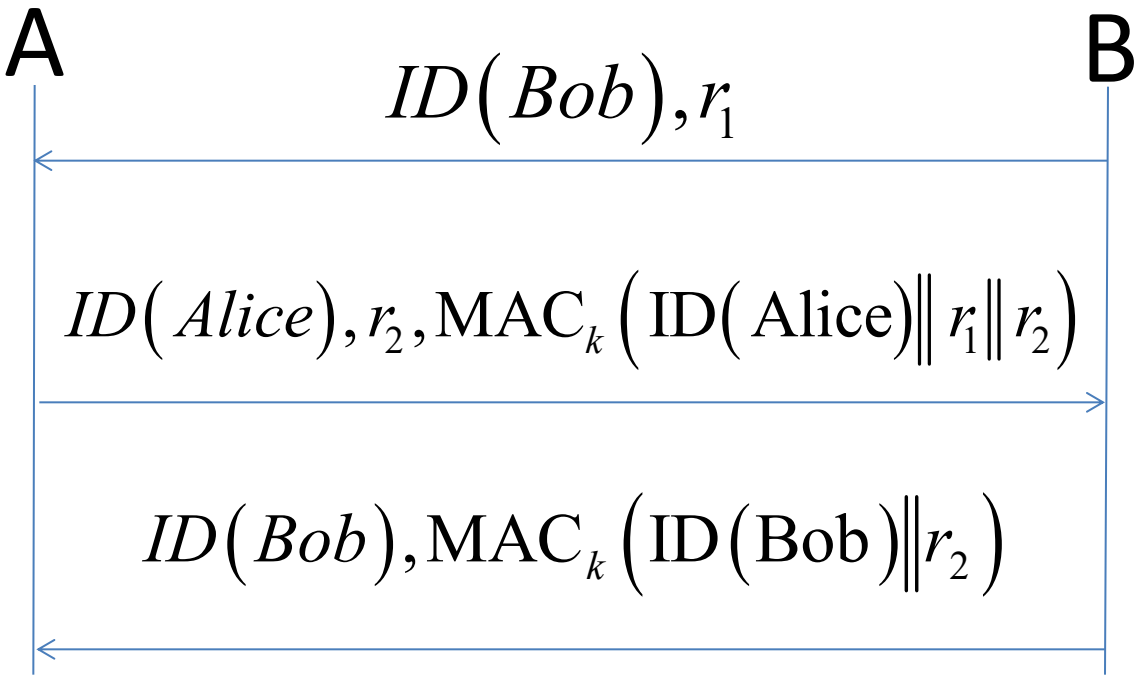


双向实体认证协议攻击


A
C
B
$ID(Bob), r_1$
$ID(Alice), r_2, \mathrm{MAC}_k(\mathrm{ID}(\mathrm{Alice}) \| r_1)$
$ID(Alice), r_2$
$ID(Bob), r_3, \mathrm{MAC}_k(\mathrm{ID}(\mathrm{Bob}) \| r_2)$
$\mathrm{ID}(\mathrm{Bob}), \mathrm{MAC}_k(\mathrm{ID}(\mathrm{Bob}) \| r_2)$

双向实体认证协议实例

改进的双向实体认证协议（基于对称密码算法）



实体认证

公钥环境下的挑战-响应方案

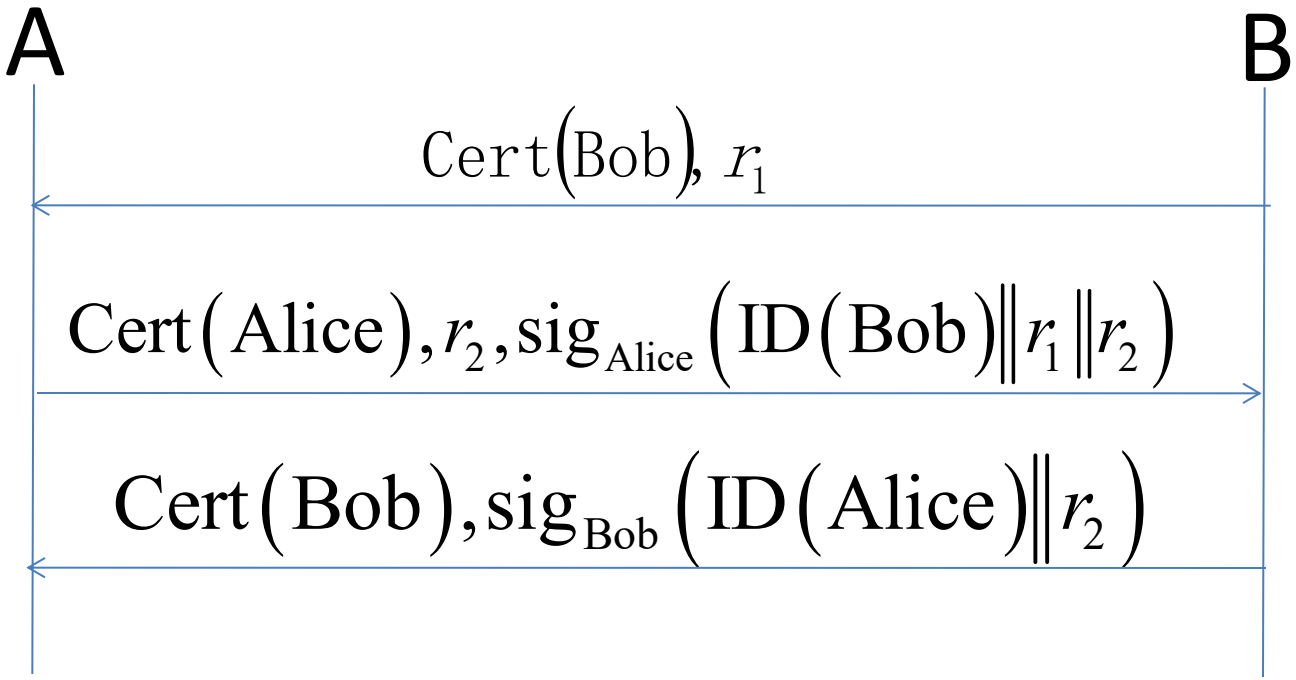
在公钥环境下，Alice和Bob没有预先的共享秘密密钥。然而，假定他们针对特定的密码体制以及签名方案，他们都有相应的公钥和私钥。

此时，用户通过公钥基础设施(Public Key Infrastructure)，向认证中心(Cerificate Authority)出示身份证明文件以及证书颁发申请，由后者制作证书后颁发给该用户。注意公钥和私钥在客户端生成，CA只是通过签名认证用户提交的公钥。

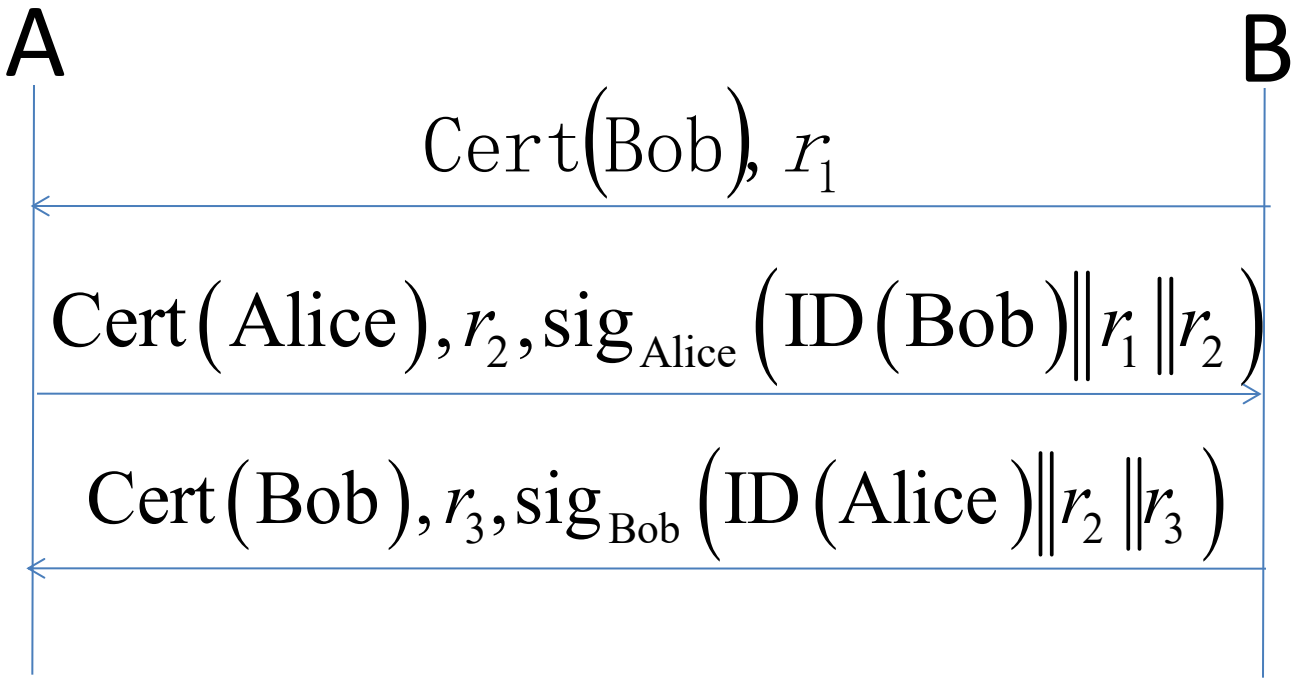
证书颁发可以在线进行也可以离线进行。

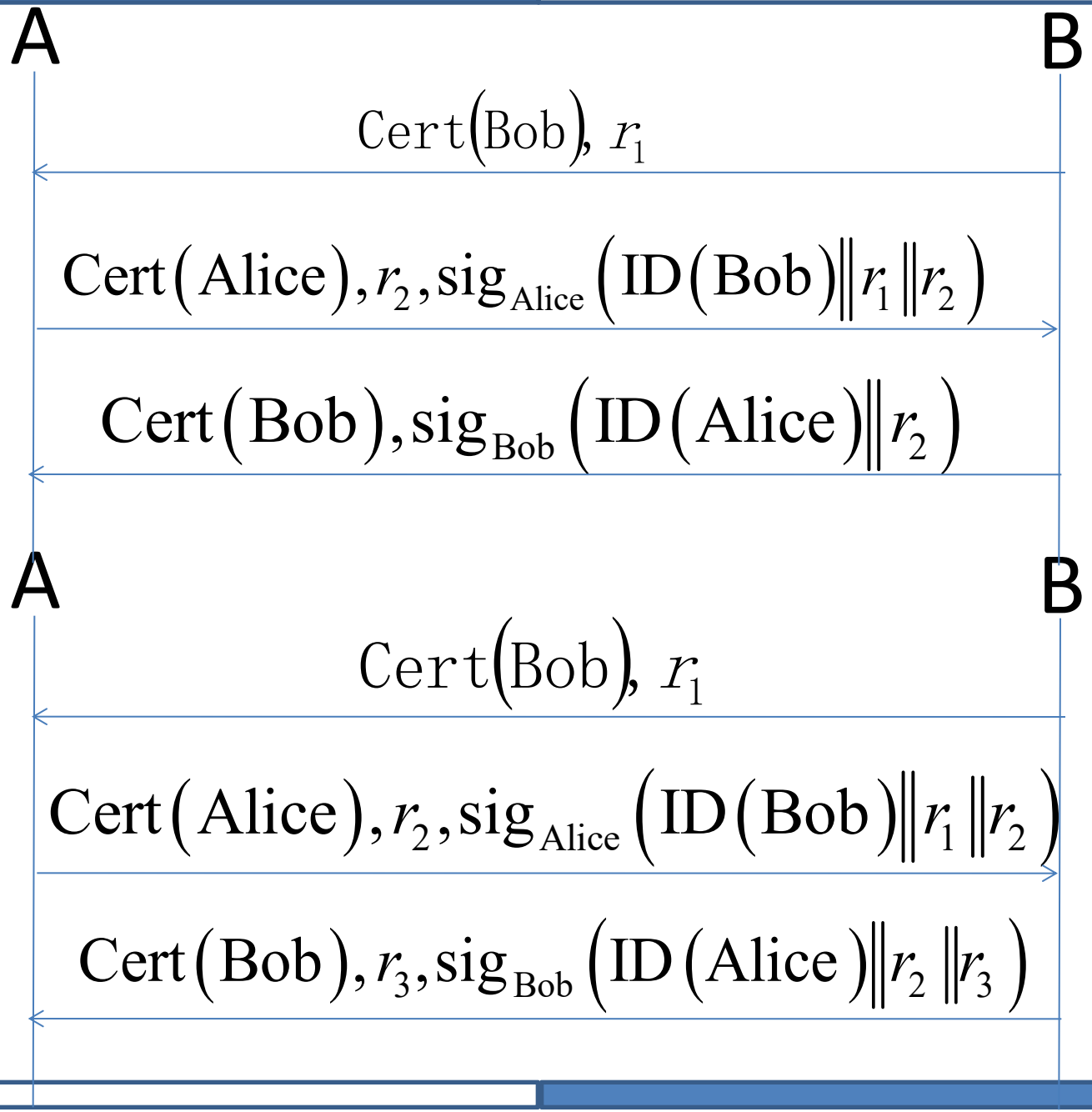
双向实体认证协议实例

改进的双向实体认证协议（基于对称密码算法）

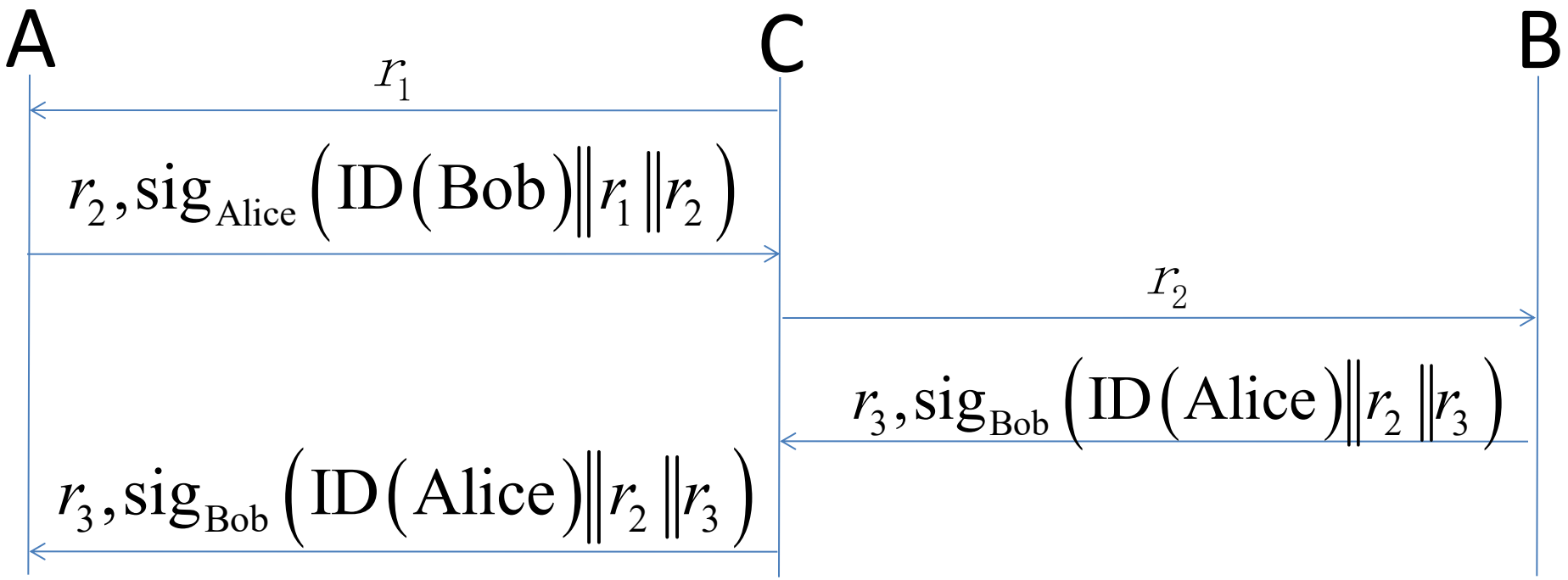


不安全的双向实体认证协议

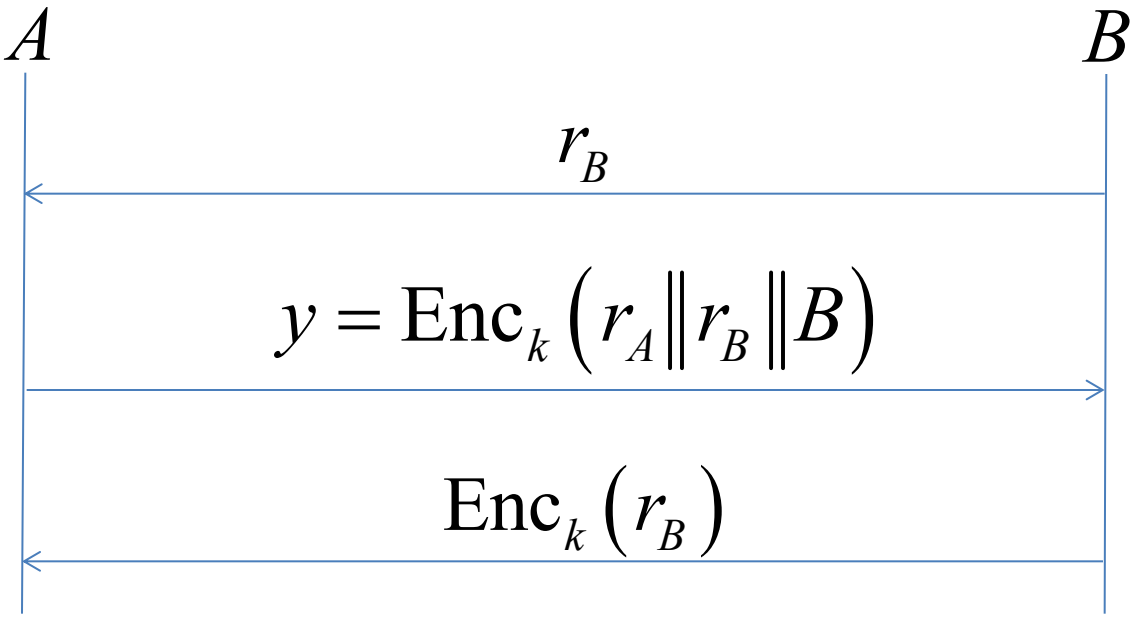



A
B
Cert(Bob), r_1
Cert(Alice), r_2, $\text{sig}_{\text{Alice}}(\text{ID}(\text{Bob}) \| r_1 \| r_2)$
Cert(Bob), $\text{sig}_{\text{Bob}}(\text{ID}(\text{Alice}) \| r_2)$
A
B
Cert(Bob), r_1
Cert(Alice), r_2, $\text{sig}_{\text{Alice}}(\text{ID}(\text{Bob}) \| r_1 \| r_2)$
Cert(Bob), r_3, $\text{sig}_{\text{Bob}}(\text{ID}(\text{Alice}) \| r_2 \| r_3)$

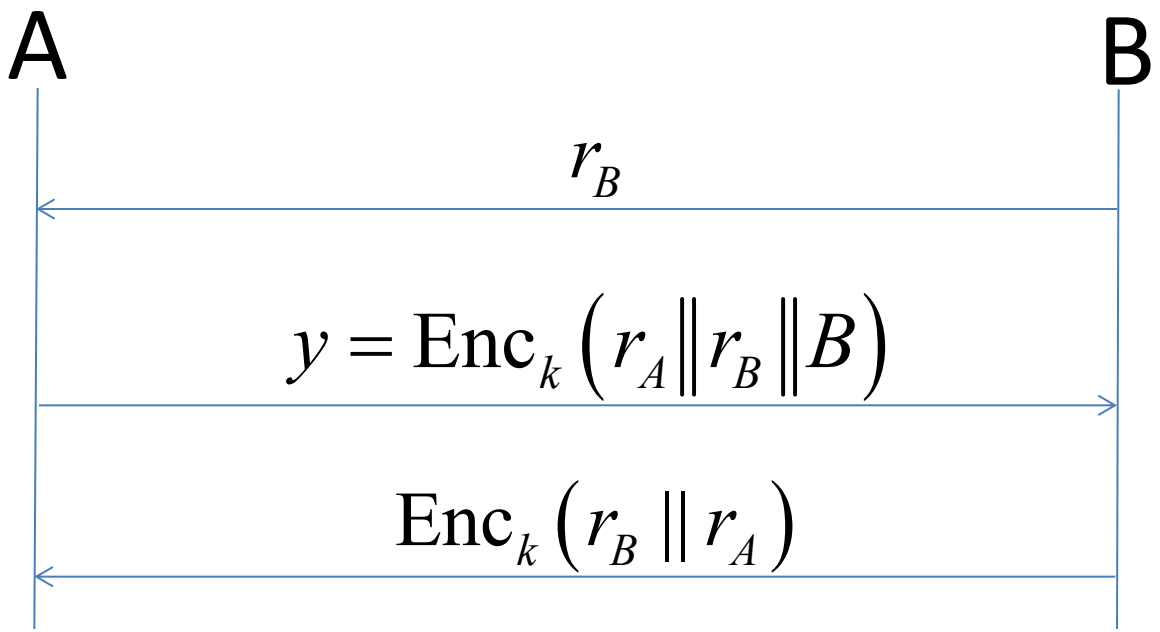
双向实体认证协议的攻击实例



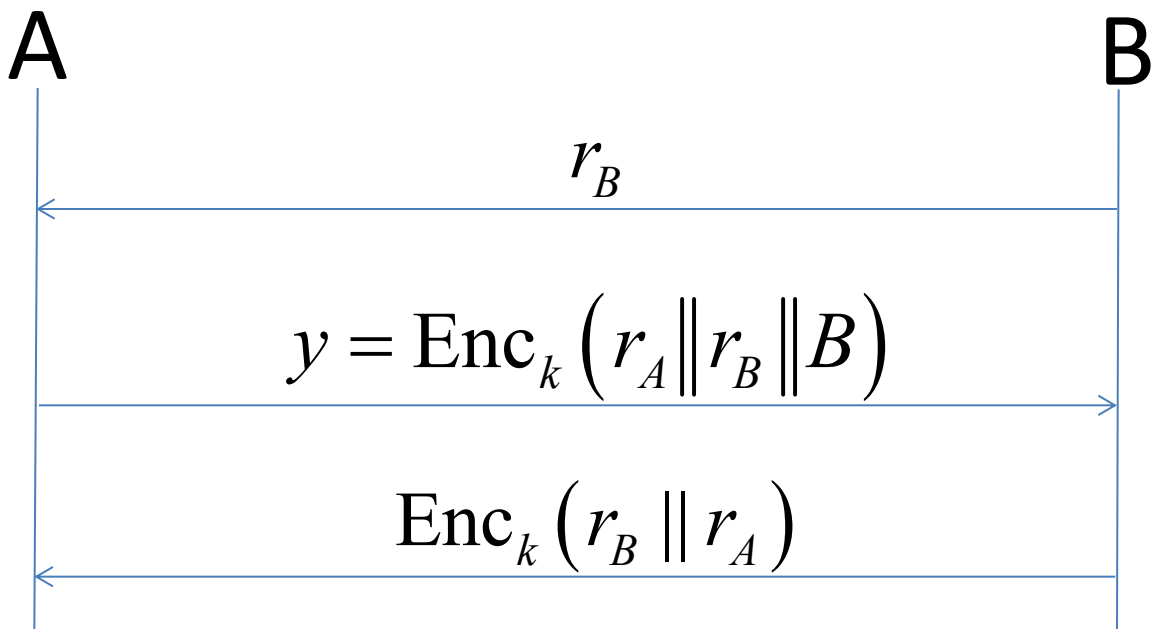
寻找攻击练习


A
B
r_B
$y = \mathrm{Enc}_k\left(r_A \| r_B \| B\right)$
$\mathrm{Enc}_k\left(r_B\right)$

寻找攻击练习


A
B
r_B
$y = \mathrm{Enc}_k\left(r_A \| r_B \| B\right)$
$\mathrm{Enc}_k\left(r_B \| r_A\right)$

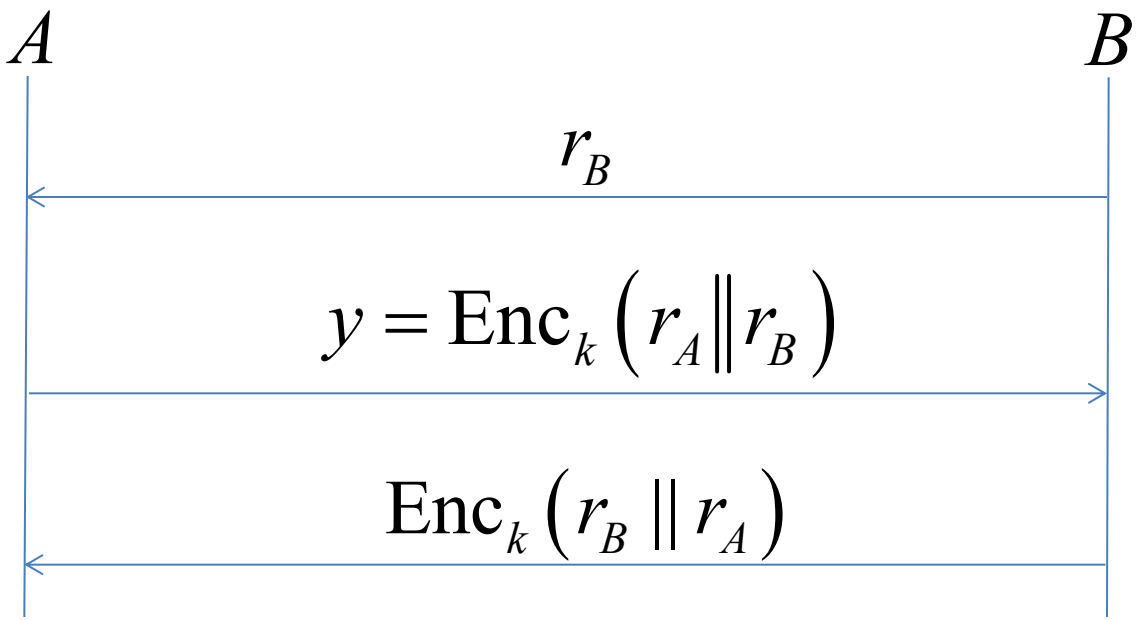
寻找攻击练习



ISO 9798-2

不是只有消息认证码算法或数字签名算法才可以用于实体认证

寻找攻击练习


A
B
r_B
$y = \mathrm{Enc}_k\left(r_A \| r_B\right)$
$\mathrm{Enc}_k\left(r_B \| r_A\right)$

More Cryptographic Protocols

实体认证（身份认证）

密钥协商

比特承诺

秘密共享

不经意传输

零知识证明