




基于公钥的密钥协商协议


南开大学网络空间安全学院

汪 定

内容提纲

- 
- 基于公钥的密钥协商协议简介
 - 采用显式认证方式的密钥协商协议
 - 采用隐式认证方式的密钥协商协议
 - 基于身份的密钥协商协议

内容提纲

- 
- 基于公钥的密钥协商协议简介
 - 采用显式认证方式的密钥协商协议
 - 采用隐式认证方式的密钥协商协议
 - 基于身份的密钥协商协议

密钥协商协议(Key Agreement Protocol)

❖ 密钥协商协议的定义：

一个密钥协商协议是一种密钥建立的方法，使得两个或者多个用户通过各自不同的输入建立一个公共的秘密值，并且任何用户不能预先确定该秘密值。

❖ 密钥协商协议的优势：

密钥建立的方式更公平，因此有利于会话密钥的随机性；

有利于实现前向安全性。

密钥控制(Key Control)

❖ 密钥控制的定义：

密钥控制用来刻画协议的参与者选择或者影响共享的秘密值的能力，通常要求任何人都不能控制密钥的产生。

❖ 密钥控制的优势：

每一个参与者产生密钥的时候不需要完全依赖于别的参与者，从而保证了密钥的随机性；

每个人有自己的输入，可以保证密钥的新鲜性。

公钥密码体制

❖ 公钥密码体制的优势：

利用公钥签名体制可以方便的实现认证；
密钥管理非常方便，不需要在线的可信中心；
适用于分布式的通信环境。

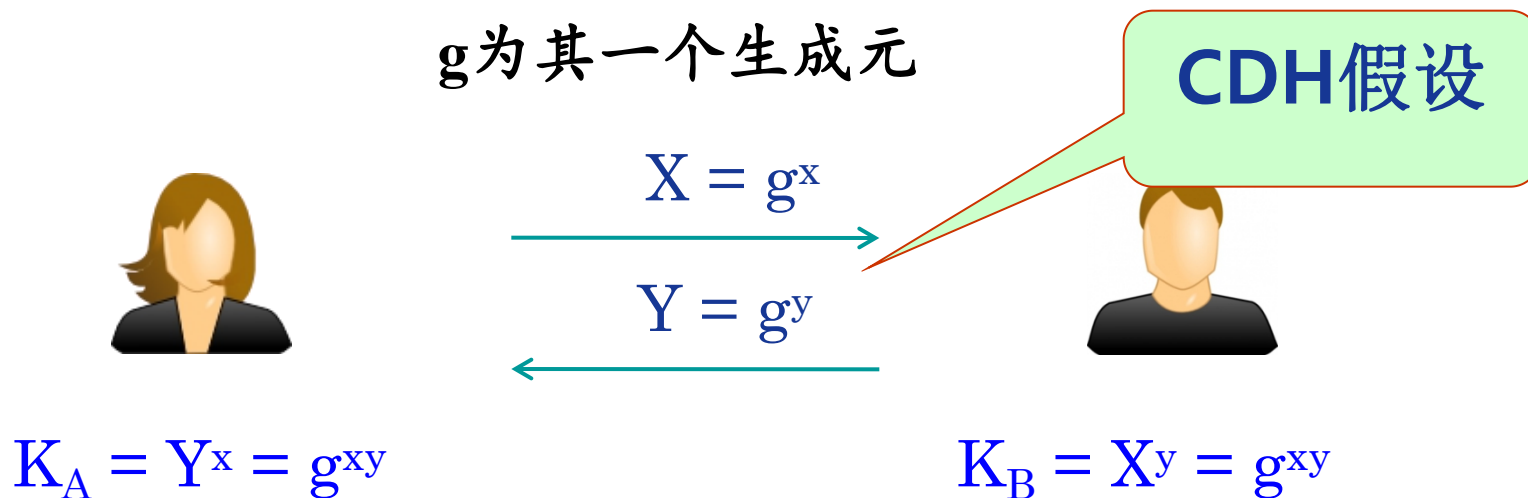
❖ 公钥密码体制的劣势：

计算量大，计算效率低；
证书管理问题（如撤销）仍然是一大难题。

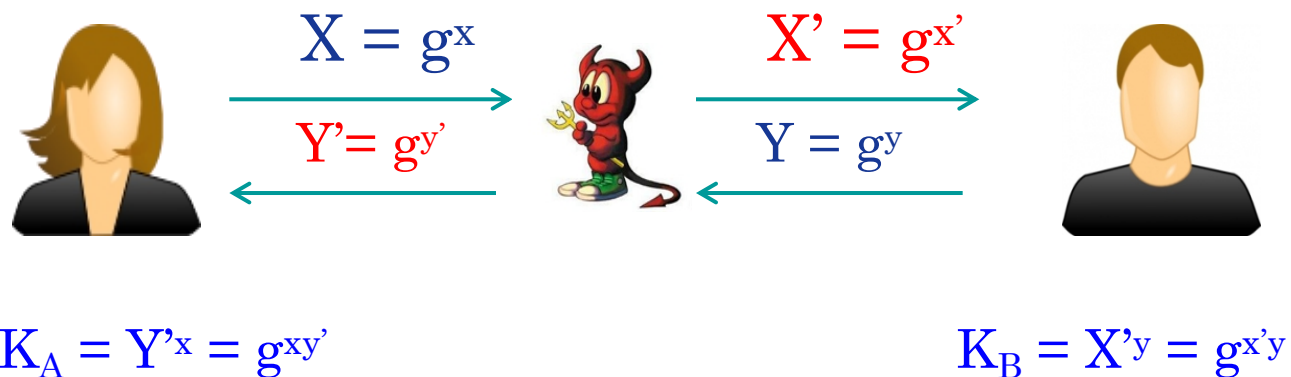
Diffie-Hellman密钥协商协议

❖ DH密钥协商协议：由著名密码学家Diffie和Hellman在1976年提出。几乎是所有密钥协商协议的基础。

设 G 是一个阶为大素数 q 的乘法循环群
 g 为其一个生成元



对DH密钥协商协议的中间人攻击



❖ 攻击者可以分别计算出 K_A 和 K_B



常用的符号

- 一些符号

p 大素数

q 素数, $q|(p-1)$

G Z_p^* 的子群

g G 的生成元

r_A, r_B A、B在 Z_q 中选择的随机数

t_A, t_B $t_A = g^{r_A}, t_B = g^{r_B}$

x_A, x_B A、B 的私钥

y_A, y_B $y_A = g^{x_A}, y_B = g^{x_B}$

K_{AB} 会话密钥

S_{AB} 静态DH密钥 $g^{x_A x_B}$

N_A, N_B A、B选择的nonces

$H()$ 单向函数

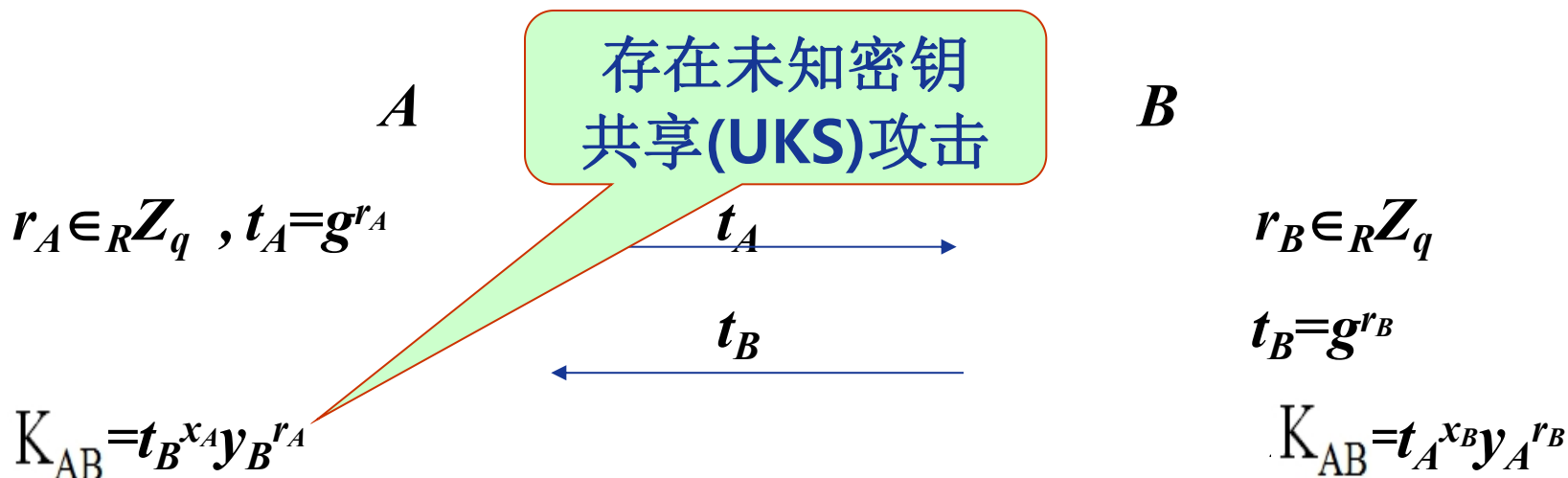
$x \in_R X$ 从 X 中随机选择 x

$F \stackrel{?}{=} G$ 验证 F 与 G 是否相等

MTI密钥协商协议

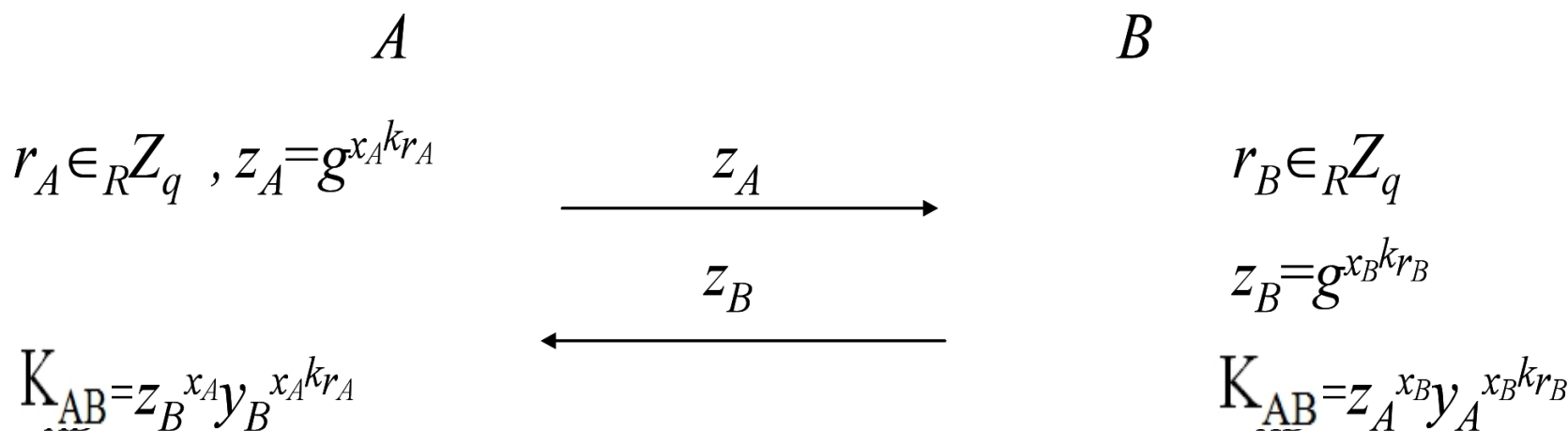
- ❖ **M**atsumoto, **T**akashima以及**I**mai(MTI)在1986年提出的三类密钥协商协议。
- ❖ 思想：将用户的长期密钥和临时密钥绑定。
- ❖ MTI协议**存在安全缺陷**，是不安全的。

MTI A(0)协议(两轮交换)



MTI密钥协商协议

MTI A(k)协议(两轮交换)。



MTI密钥协商协议

类型	z_A	z_B	K_{AB}	A计算	B计算
A(0)	g^{r_A}	g^{r_B}	$g^{x_A r_B + x_B r_A}$	$z_B^{x_A} y_B^{r_A}$	$z_A^{x_B} y_A^{r_B}$
B(0)	$y_B^{r_A}$	$y_A^{r_B}$	$g^{r_A + r_B}$	$z_B^{x_A - 1} g^{r_A}$	$z_A^{x_B - 1} g^{r_B}$
C(0)	$y_B^{r_A}$	$y_A^{r_B}$	$g^{r_A r_B}$	$z_B^{x_A - 1} r_A$	$z_A^{x_B - 1} r_B$

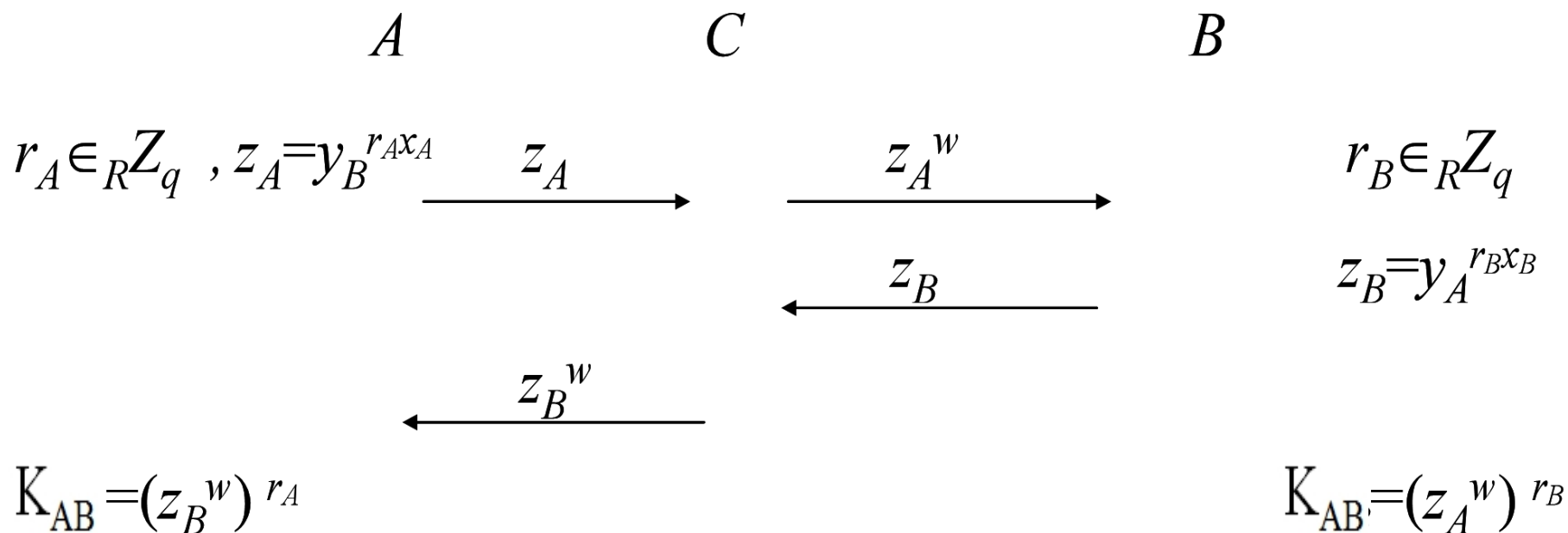
MTI密钥协商协议

k	$A(k)$	$B(k)$	$C(k)$
-1	$x_A x_B^{-1} r_B + x_B x_A^{-1} r_A$	$x_A^{-1} r_A + x_B^{-1} r_B$	$x_A^{-1} r_A x_B^{-1} r_B$
0	$x_A r_B + x_B r_A$	$r_A + r_B$	$r_A r_B$
1	$x_A x_B r_B + x_B x_A r_A$	$x_A r_A + x_B r_B$	$x_A r_A x_B r_B$
...
K	$x_A x_B^k r_B + x_B x_A^k r_A$	$x_A^k r_A + x_B^k r_B$	$x_A^k r_A x_B^k r_B$

对MTI协议的小子群攻击

对MTI C(1)协议的小子群攻击

共享信息： Z_p^* 的生成元 g 。 $P-1$ 的小因子 r ， $w=(p-1) / r$

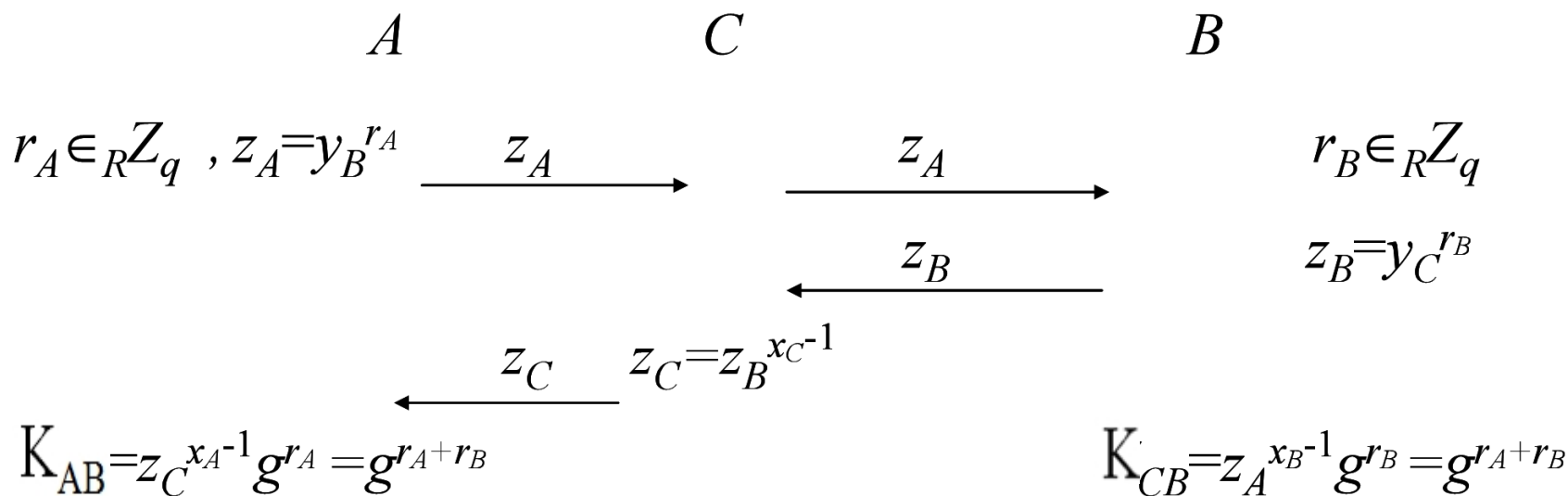


对MTI协议的未知密钥共享攻击

对 MTI B(0)协议的未知密钥共享攻击

共享信息: C的公钥 $y_C = y_A^{x_C}$ 。

C不知道A的
私钥



如何令MTI协议能够抵抗未知密钥共享攻击?

增加私钥证明, 在会话密钥中增加身份

Menezes等人的改进协议

修改的MTI B(0)协议

共享信息：哈希函数H。

A

B

$$r_A \in_R \mathbb{Z}_q, z_A = y_B^{r_A}$$

z_A

$$r_B \in_R \mathbb{Z}_q$$

z_B, h

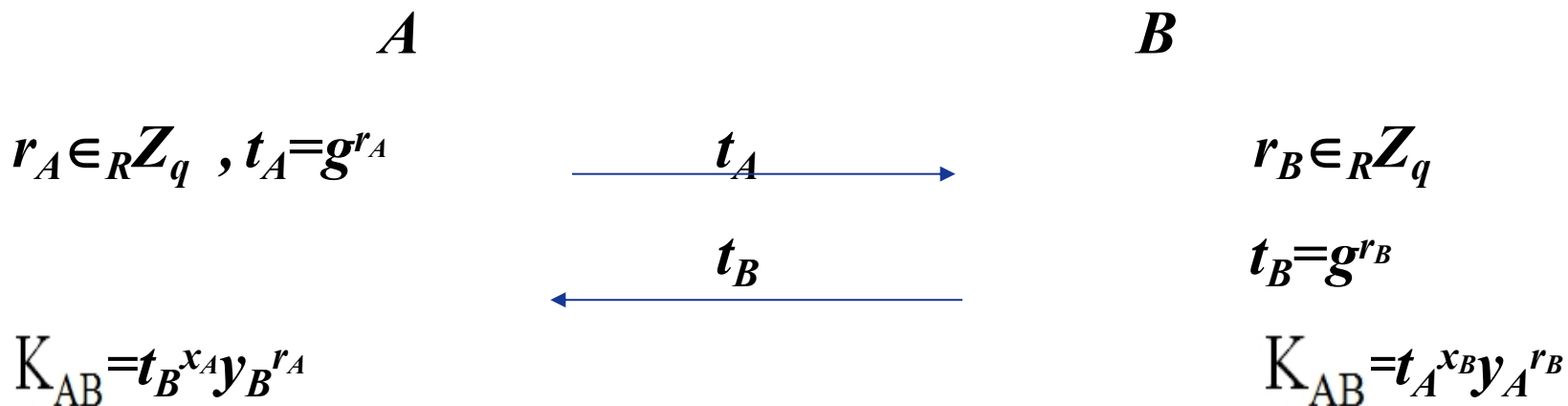
$$z_B = y_A^{r_B}, K_{AB} = z_A^{x_B^{-1}} g^{r_B}$$

$$K_{AB} = z_B^{x_A^{-1}} g^{r_A}, H(z_B, K_{AB}) \stackrel{?}{=} h$$

$$h = H(z_B, K_{AB})$$

MTI协议的前向安全性

MTI A(0)协议(两轮交换)



类型	z_A	z_B	K_{AB}	A计算	B计算
A(0)	g^{r_A}	g^{r_B}	$g^{x_A r_B + x_B r_A}$	$z_B^{x_A} y_B^{r_A}$	$z_A^{x_B} y_A^{r_B}$
B(0)	$y_B^{r_A}$	$y_A^{r_B}$	$g^{r_A + r_B}$	$z_B^{x_A - 1} g^{r_A}$	$z_A^{x_B - 1} g^{r_B}$
C(0)	$y_B^{r_A}$	$y_A^{r_B}$	$g^{r_A r_B}$	$z_B^{x_A - 1} r_A$	$z_A^{x_B - 1} r_B$

对MTI协议的密钥泄漏仿冒攻击

对MTI C(0)协议的密钥泄露仿冒攻击

条件：C知道A的私钥 x_A 。

A

B(C)

$$r_A \in_R \mathbb{Z}_q, z_A = y_B^{r_A}$$

z_A

$$r_C \in_R \mathbb{Z}_q, z_B = y_B^{x_A r_C}$$

z_B


$$K_{AB} = z_B^{x_A^{-1} r_A} = y_B^{r_A r_C}$$

$$K_{AB} = z_A^{r_C} = y_B^{r_A r_C}$$

基于公钥的密钥协商协议的安全需求

- ❖ 1. 抗已知密钥攻击 (Known key attack)
- ❖ 2. 实现前向安全性 (Forward secrecy)
- ❖ 3. 抵抗密钥泄漏仿冒攻击 (KCI)
- ❖ 4. 抵抗未知密钥共享攻击 (UKS)
- ❖ 5. 抵抗临时密钥泄漏 (Empheral leakage)
- ❖ 6. 实现密钥控制 (Key control)
- ❖ 匿名性, 可证明安全性, . . .

内容提纲

- 
- 基于公钥的密钥协商协议简介
 - 采用显式认证方式的密钥协商协议
 - 采用隐式认证方式的密钥协商协议
 - 基于身份的密钥协商协议

显式认证的密钥协商协议

❖对DH密钥交换改进的思路：

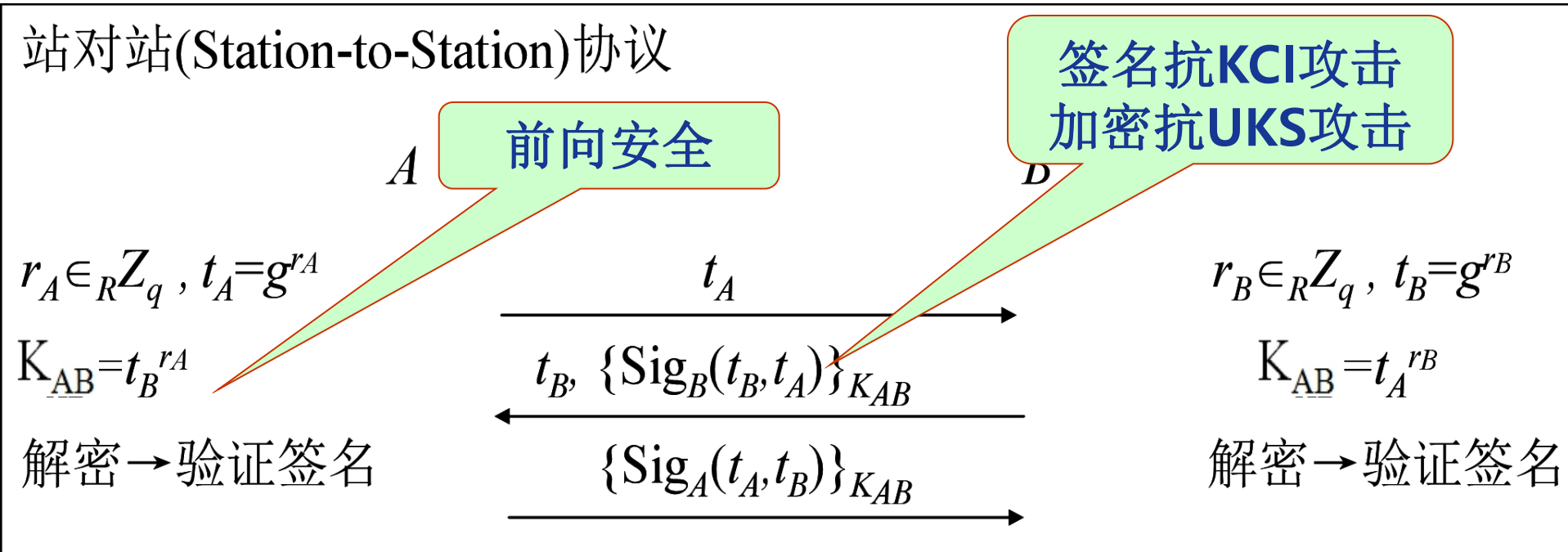
通过签名等方式增加认证。

最终的共享密钥是临时的DH密钥值，因此可以实现前向安全性；

临时的DH公钥由长期密钥进行签名，因此可以抵抗密钥泄漏仿冒攻击。

STS协议(Station to Station)

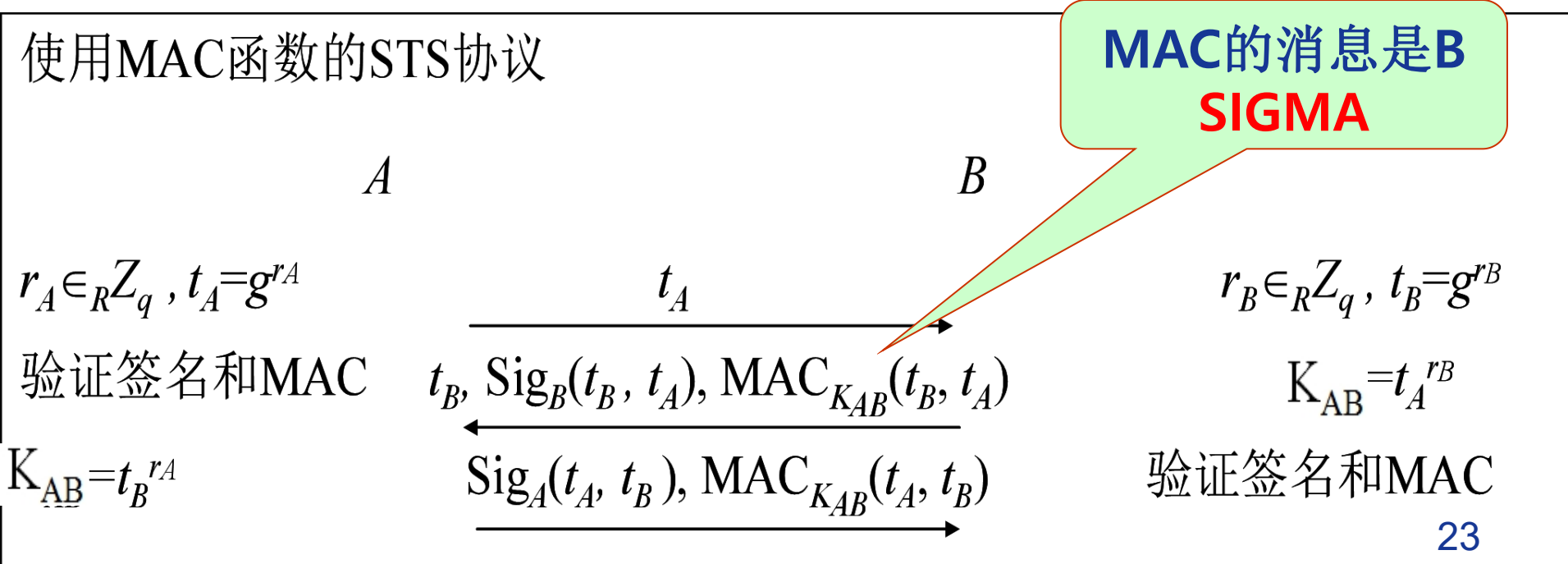
❖ STS协议由Diffie等人在1992年提出，主要的思想是通过签名来克服DH协议缺乏认证的不足。



使用MAC函数的STS协议

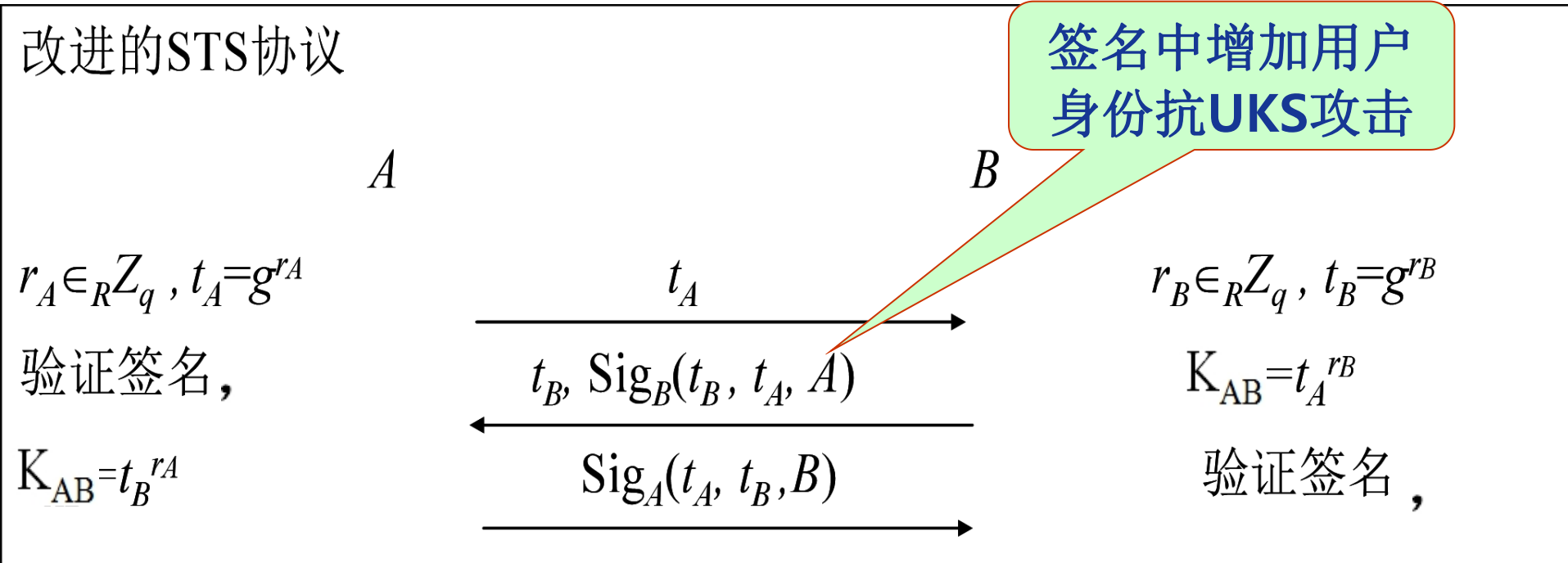
❖ STS协议中通过加密来抵抗未知密钥共享攻击。但是这里参与者只需要证明自己知道会话密钥。

真正需要的是认证！



改进的STS协议

❖ 改进的STS协议在著名的CK模型下是可证明安全的。



Arazi的密钥协商协议

- ❖ Arazi设计了一个将DH密钥交换以及DSS签名结合的密钥协商协议。
- ❖ 将DH密钥交换中的随机数复用，即用于密钥交换也用于生成DSS签名的随机数。
- ❖ 设计精巧并且协议高效，但是存在安全性方面的不足。

Arazi的密钥协商协议

Arazi的密钥协商协议

A

B

$$r_A \in_R Z_q, t_A = g^{r_A}$$

$$s_A = r_A^{-1} (H(t_A) + x_A t_A) \bmod q$$

t_A, s_A

$$\text{验证签名, } r_B \in_R Z_q, t_B = g^{r_B}$$

$$s_B = r_B^{-1} (H(t_B) + x_B t_B) \bmod q$$

t_B, s_B

$$\text{验证签名, } K_{AB} = t_B^{r_A}$$

$$K_{AB} = t_A^{r_B}$$

是否能抗重放攻击？临时密钥泄露攻击？

Lim-Lee的密钥协商协议

Lim-Lee基于Schnorr签名的协议

A

B

$$r_A \in_R \mathbb{Z}_q, t_A = g^{r_A}$$

$$\xrightarrow{t_A}$$

$$r_B \in_R \mathbb{Z}_q, t_B = g^{r_B}, E = H(t_A, t_B)$$

$$\xleftarrow{s_B, E}$$

$$s_B = (r_B - x_B E) \bmod q$$

$$t_B = g^{s_B} y_B^E, E \stackrel{?}{=} H(t_A, t_B)$$

$$K_{AB} = t_A^{r_B}$$

$$s_A = (r_A - x_A E) \bmod q$$


$$\xrightarrow{s_A}$$

$$g^{s_A} y_A^E \bmod p \stackrel{?}{=} t_A$$

$$K_{AB} = t_B^{r_A}$$

是否具有前向安全性？为什么协议是三轮的？

内容提纲

- 
- 基于公钥的密钥协商协议简介
 - 采用显式认证方式的密钥协商协议
 - 采用隐式认证方式的密钥协商协议
 - 基于身份的密钥协商协议

隐式认证的密钥协商协议

❖对DH密钥交换改进的思路：

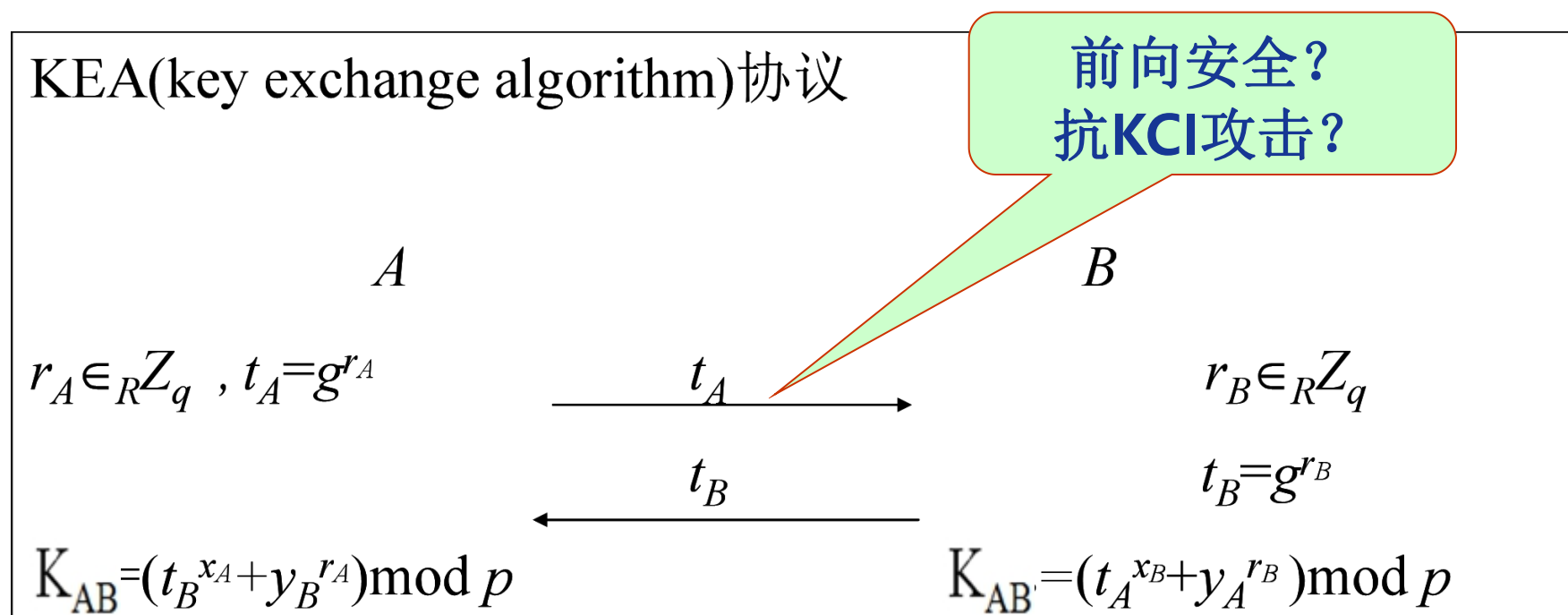
消息的格式与原始的DH协议相同，通过共享密钥的计算方式实现隐式认证。

最终的共享密钥是参与者长期密钥与临时密钥结合产生的；

MTI系列协议属于隐式认证的密钥协商协议。

KEA密钥协商协议

❖ KEA协议是由美国国家安全局设计的，可以看做是MTIA(0)协议的变形。



MQV协议

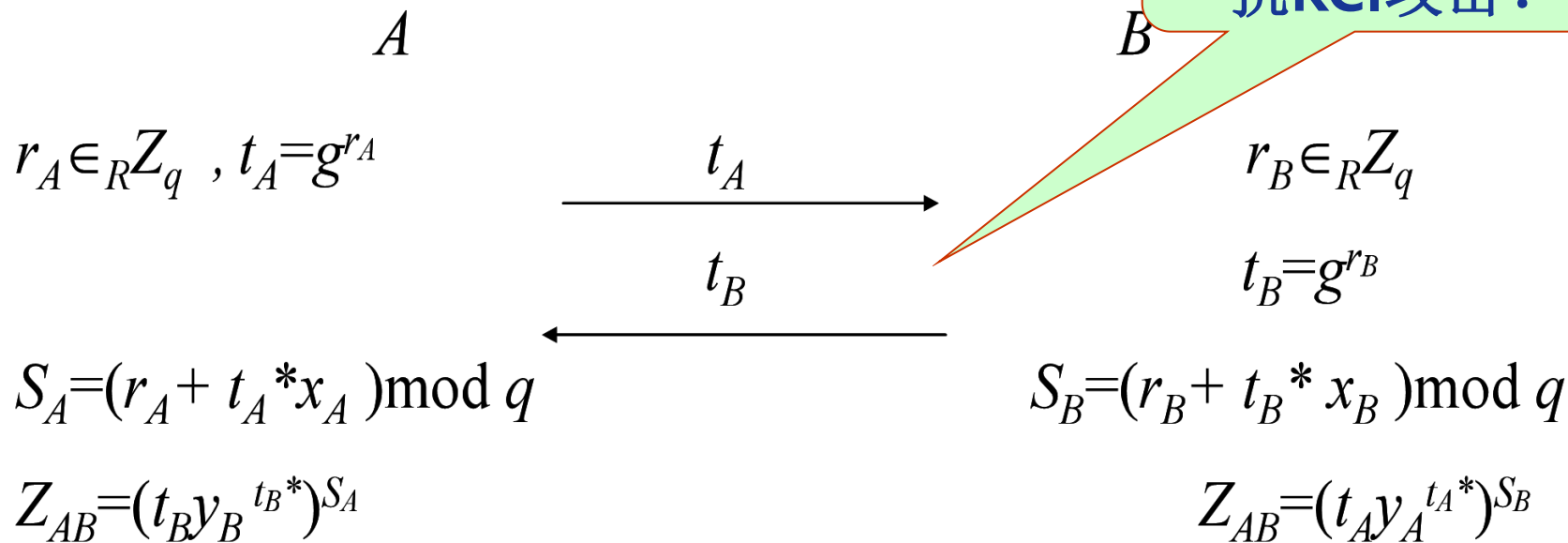
- ❖ MQV协议是Menezes等人最早在1995年提出的，在2003年作者又进行了改进。
- ❖ MQV协议被多个标准化组织列为密钥协商协议的标准，如ANSI、IEEE P1363和NSA等。In 2004, NSA chose it as “the next generation cryptology to protect US government information”
- ❖ 思想：通过DH临时公钥产生特殊的参数用于会话密钥的生成。

MQV协议

MQV(Menezes-Qu-Vanstone)协议(IEEE P1363-2000)

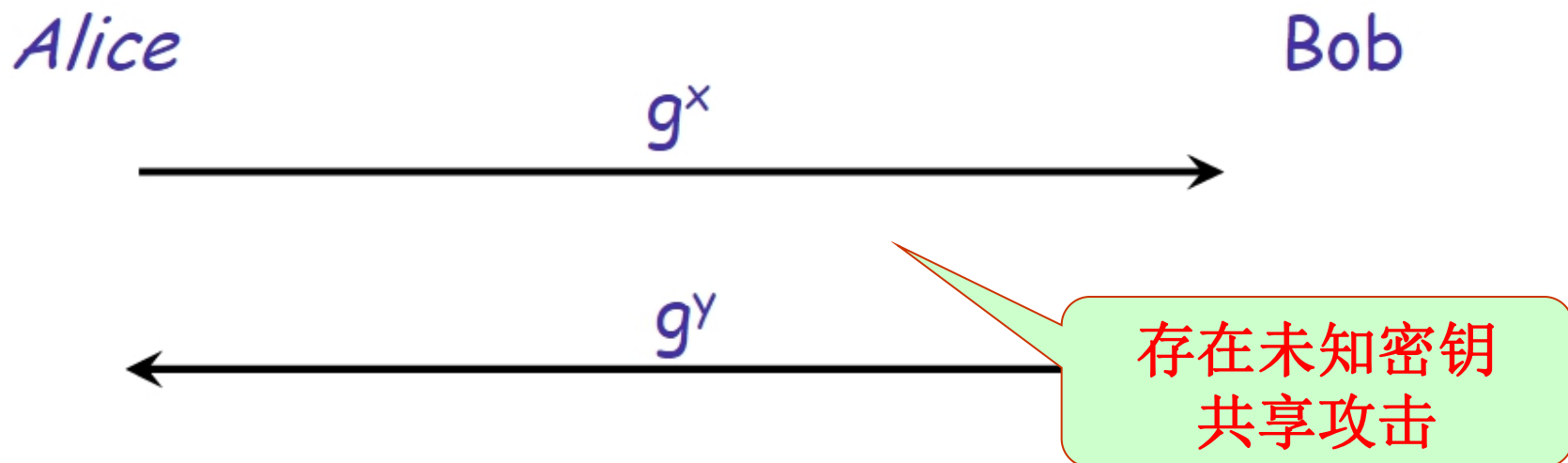
共享信息: $t^* = t \bmod 2^w + 2^w$, $\# \langle G \rangle = q$ (素数), $q | (p-1)$

前向安全?
抗KCI攻击?



设计思想精巧！效率奇高！

MQV协议



- As basic DH ($X=g^x, Y=g^y$), PKs: $A=g^a, B=g^b$
- Both compute $\sigma=g^{(x+da)(y+eb)}$ as $\sigma = (YB^e)^{x+da} = (XA^d)^{y+eb}$
- $d = 2^\ell + (X \bmod 2^\ell)$, $e = 2^\ell + (Y \bmod 2^\ell)$, $\ell = |q|/2$.
- Session key $K=H(\sigma)$

对MQV协议的未知密钥共享攻击

$$\hat{A} \quad A = g^a$$

$$\xrightarrow{\hat{A}, X = g^x}$$

$$\hat{C} \quad C = g^c$$

$$z \in_R \mathbb{Z}_2;$$

$$Z = X A^d g^{-z};$$

$$c = f^{-1} z \bmod 2;$$

$$C = g^c;$$

$$\hat{B} \quad B = g^b$$

$$\xrightarrow{\hat{C}, Z = X A^d g^{-z}}$$

$$y \in_R \mathbb{Z}_2;$$

$$Y = g^y;$$

$$\xleftarrow{\hat{B}, Y = g^y}$$

$$\xleftarrow{\hat{B}, Y = g^y}$$

$$K_{AB} = (Y B^e)^{x+da}$$

$$K_{CB} = (Z C^f)^{y+eb}$$

$$= (X A^d g^{-z} \cdot g^{f^{-1} z \cdot f})^{y+eb}$$

$$= (X A^d)^{y+eb}$$

其中, d, e, f 都是公开可计算的:

$$d = 2^l + (X \bmod 2^l); \quad || l = \frac{|Q|}{2}$$

$$e = 2^l + (Y \bmod 2^l);$$

$$f = 2^l + (Z \bmod 2^l);$$

HMQV协议

- ❖ **HMQV**协议是Krawczyk在2005年提出的对**MQV**协议的一种变形。
- ❖ **MQV**协议虽然被多个标准化组织确认为标准，但是没有严格的安全证明。
- ❖ 利用**Schnorr**身份验证协议对**MQV**进行了改进，保持了**MQV**协议的所有优点，并且是可证明安全的。
- ❖ **HMQV**协议是目前为止效率和安全综合性能最好的密钥协商协议。

XCR签名

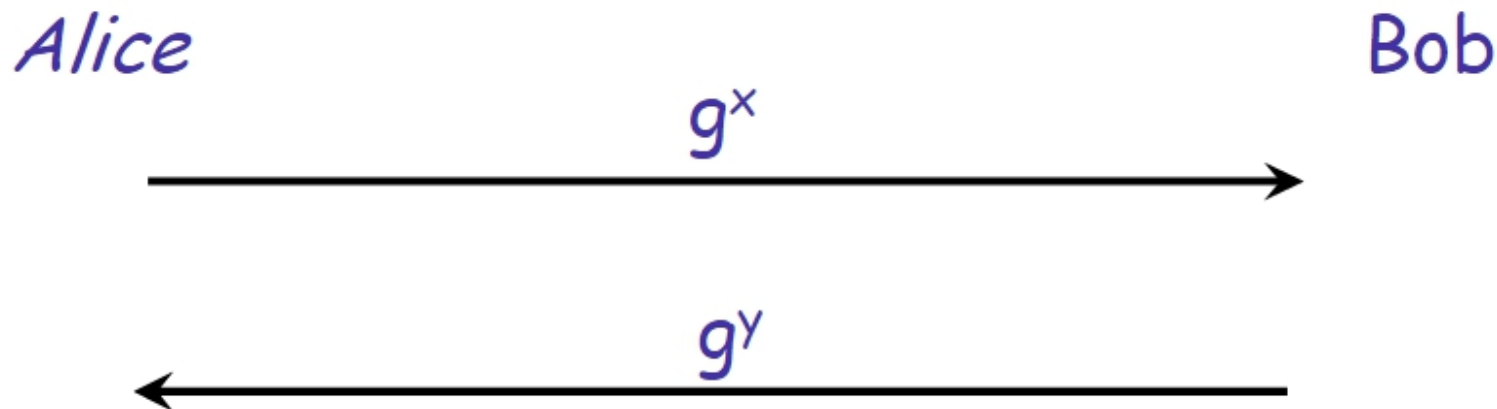
❖ XCR (Exponential Challenge-Response) 签名是一个交互式的签名。签名者Bob拥有私钥 b 和对应的公钥 $B=g^b$ 。验证者Alice提供一个消息 m 和挑战 $X=g^x$ ，想要让Bob产生签名。

1、Alice发送挑战 X 和消息 m 给Bob。

2、Bob随机选择 y 并计算 $Y=g^y$ ，计算签名 $X^{y+H(Y, m)b}$ ，发送 Y 和签名给Alice。


3、Alice通过 $(YB^{H(Y, m)})^x$ 是否等于签名来验证签名的有效性。

HMQV协议



- As basic DH ($X=g^x$, $Y=g^y$), PKs: $A=g^a$, $B=g^b$
- Both compute $\sigma=g^{(x+da)(y+eb)}$ as $\sigma = (YB^e)^{x+da} = (XA^d)^{y+eb}$
- $d=H(X, \text{"Bob"})$ $e=H(Y, \text{"Alice"})$ (here H outputs $|q|/2$ bits)
- Session key $K=H(\sigma)$

内容提纲

- 
- 基于公钥的密钥协商协议简介
 - 采用显式认证方式的密钥协商协议
 - 采用隐式认证方式的密钥协商协议
 - 基于身份的密钥协商协议

基于身份的密钥协商协议

- ❖ 用基于身份的公私钥对来代替基于**PKI**的公私钥对。一般基于身份的公私钥对是由**可信的密钥生成中心PKG**生成的。
- ❖ **PKG**: sP P 是**G**的生成元 **G**是阶为大素数 q 的循环群
- ❖ 对于用户**ID**，其公钥为**H(ID)**，**PKG**为其生成私钥**sH(ID)**

基于身份的密钥协商协议的安全性需求

- ❖ 1. 已知密钥安全(**known-key security**): 一次会话的密钥泄漏不会影响其他会话
- ❖ 2. 前向安全: 用户的长期密钥泄漏不会对以前的会话密钥的安全性造成威胁。基于身份的**AKE**还要考虑**PKG**的主密钥泄漏时的前向安全 (**PKG-fs**)
- ❖ 3. 抵抗**KCI**攻击
- ❖ 4. 抵抗临时密钥泄漏
- ❖ 5. 抵抗**UKS**攻击
- ❖ 6. 实现密钥控制

Okamoto的基于身份的密钥协商协议

❖ Okamoto的协议是第一个基于身份的密钥协商协议。

PKG的公钥

Okamoto的基于身份密钥协商协议

共享信息：公开模数 $n=pq$ 和加密指数 e ;

$g \in Z_n^*$; g 同时是 Z_p^* 和 Z_q^* 的生成元。

A 的私钥: s_A : $s_A^e = ID_A^{-1} \bmod n$; B 的私钥: s_B : $s_B^e = ID_B^{-1} \bmod n$

A

B

$$r_A \in_R Z_n, t_A = g^{r_A}$$

$$Z_{AB} = ((s_B t_B)^e ID_B)^{r_A}$$

$$s_A t_A$$

$$s_B t_B$$

$$r_B \in_R Z_n, t_B = g^{r_B},$$

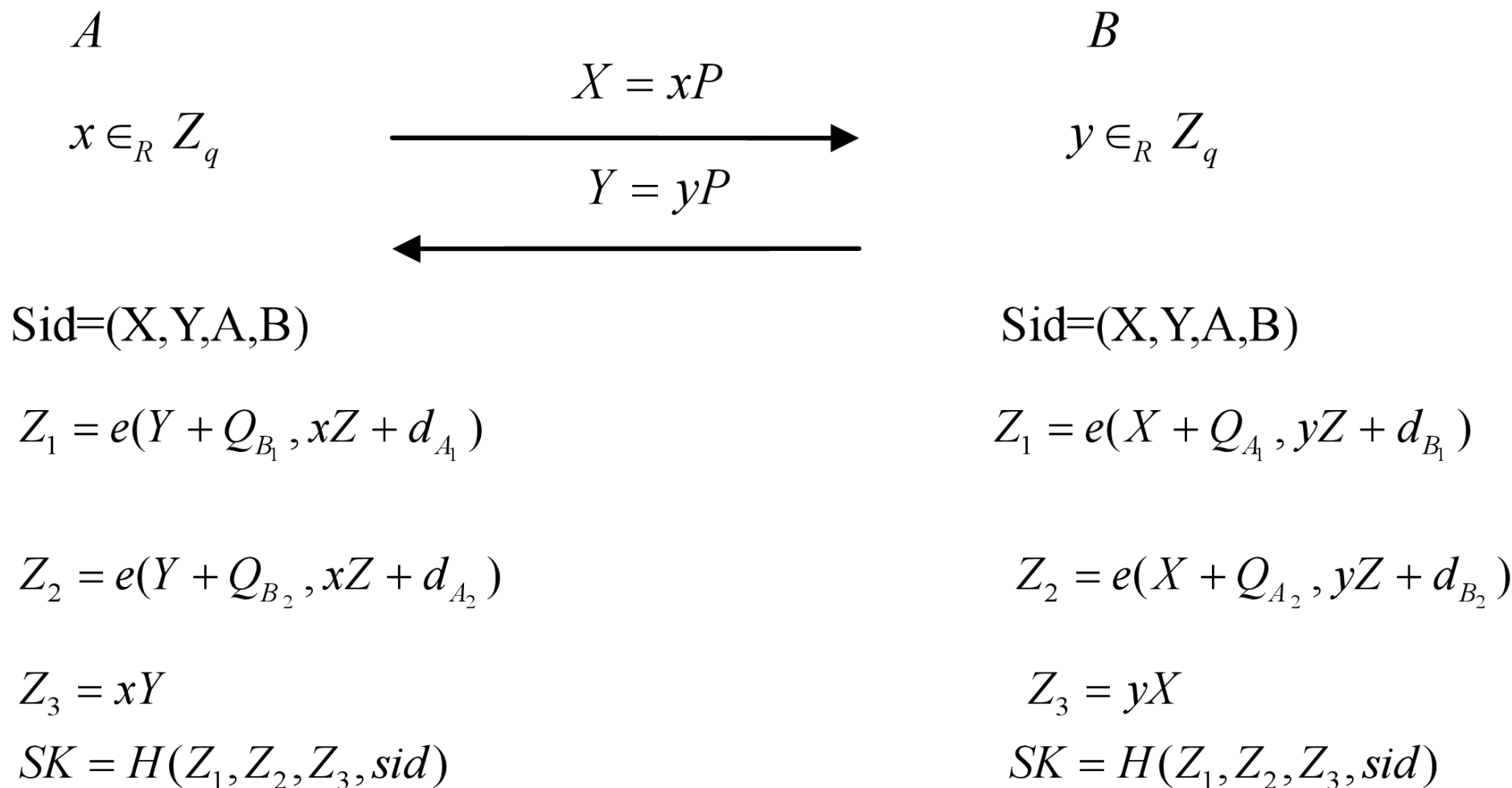
$$Z_{AB} = ((s_A t_A)^e ID_A)^{r_B}$$

基于双线性对的密钥协商协议

令 G 为阶数为素数 q 的加法循环群, G^* 为阶数为素数 q 的乘法循环群, P 为群 G 的一个生成元. 再令 $e: G \times G \rightarrow G^*$ 为满足下列性质的双线性对:

- (1) 双线性性: 对于所有的 P, Q 以及 $R \in G$ 有 $e:(P+Q, R) = e(P, R)e(Q, R)$ 以及 $e:(P, Q+R) = e(P, Q)e(P, R)$ 。
- (2) 非退化性: 存在 $P, Q \in G$ 使得 $e(P, Q) \neq 1$ 。
- (3) 可计算性: 对所有 $P, Q \in G$, 存在有效算法可以计算 $e(P, Q) \neq 1$ 。

基于双线性对的密钥协商协议





Thank You !

敬请批评指正！