

$X'_2 = X_2 g^{-pw_A}, Y'_2 = Y_2 g^{-pw_B}, \sigma_A = X_1^{\lambda_1} X_2^{\lambda_2}$ 和 $\sigma_B = Y_1^{\lambda_1} Y_2^{\lambda_2}$. 这里, λ_1 和 λ_2 为基于 ElGamal 加密算法的平滑投射函数的全局密钥, μ 是对应的投射密钥. σ_A 和 σ_B 则是服务器分别与用户 A 和 B 共享的平滑投射哈希函数的输出. 此外, 服务器 S 还选择随机数 $z \in Z_q^*$ 并计算 $X_1^* = X_1^z$ 以及 $Y_1^* = Y_1^z$. 服务器 S 计算通用哈希函数的输出 $r_A \parallel \tau_{A1} \parallel \tau_{A2} = UH(\sigma_A)$ 和 $r_B \parallel \tau_{B1} \parallel \tau_{B2} = UH(\sigma_B)$. 这里, r_A 和 r_B 分别用于 CCA 加密算法的随机输入, τ_{A1} 和 τ_{B1} 分别用作利用对称加密算法加密随机化后的密钥材料 X_1^* 以及 Y_1^* 时的密钥, 而 τ_{A2} 和 τ_{B2} 则用于实现用户向服务器的认证. 服务器 S 计算密文 $C_A = Enc_{\tau_{A1}}(Y_1^*)$ 和 $C_B = Enc_{\tau_{B1}}(X_1^*)$, 并用 r_A 和 r_B 作为随机输入, 对 $\Sigma_A = H(X_1, X'_2, C_A, \mu, A, B, S)$ 和 $\Sigma_B = H(Y_1, Y'_2, C_B, \mu, A, B, S)$ 分别进行加密得到密文 ω_A 和 ω_B . 最后, 服务器 S 分别发送消息 (S, C_A, μ, ω_A) 和 (S, C_B, μ, ω_B) 给用户 A 和 B .

第 3 轮. 用户 A 接收到消息 (S, C_A, μ, ω_A) 后, 首先利用投射密钥 μ 计算平滑投射哈希函数的输出 $\sigma_A = \mu^x$, 并计算通用哈希函数的输出 $r'_A \parallel \tau'_{A1} \parallel \tau'_{A2} = UH(\sigma_A)$; 用户 A 首先利用 τ'_{A1} 解密 C_A 得到 Y_1^* , 并验证 ω_A 是否等于 $E_{pk}[\Sigma_A, r'_A]$, 如果不相等, 则拒绝并结束协议运行; 否则, 用户 A 计算会话密钥 $K = Y_1^{*x}$ 并发送消息 (A, τ'_{A2}) 给服务器 S . 用户 B 和用户 A 执行类似的操作, 为了简便起见, 这里略去该部分描述.

最后, 服务器 S 接收到消息 (A, τ'_{A2}) 和 (B, τ'_{B2}) 后, 验证 τ'_{A2} 和 τ'_{B2} 是否有效: 如果有效, 则服务器 S 接受协议运行; 如果无效, 则说明前面的接入请求来自敌手对某个用户进行的仿冒攻击. 如果服务器没有收到消息 (A, τ'_{A2}) 或 (B, τ'_{B2}) , 则同样认为前面的接入请求来自敌手对某个用户进行的仿冒攻击, 服务器将采取进一步的措施 (如限制用户认证次数等) 以保护用户口令 (如图 1 所示).

注: 两个用户 A 和 B 在发送最后一轮消息时, 已经建立了共享的会话密钥用于后续的安全通信. 第 3 轮消息的目的在于用户向服务器证明其合法身份, 从而达到双向认证和抵抗不可检测在线字典攻击的目的.

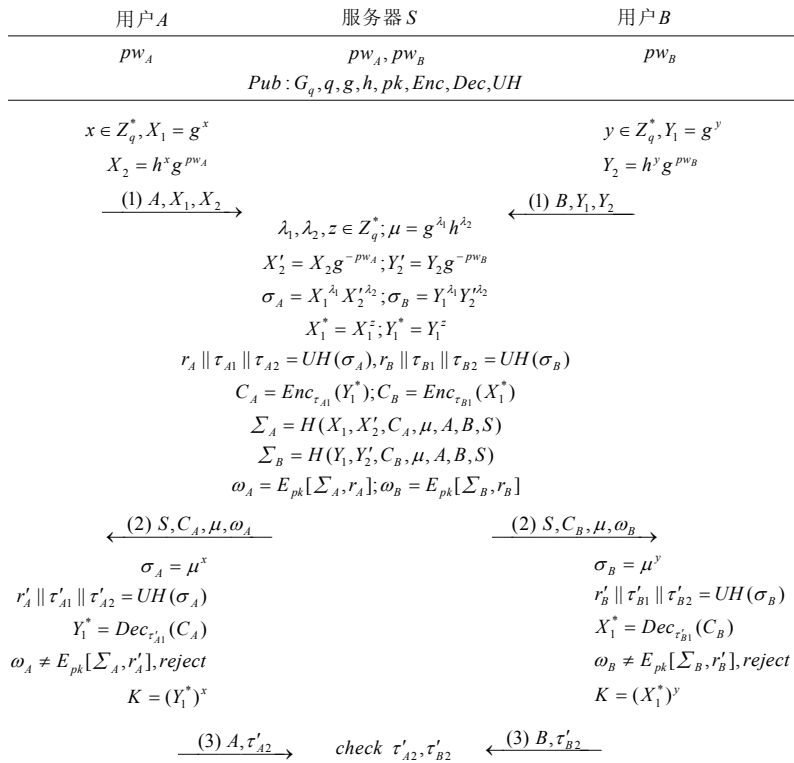


Fig. 1 An efficient 3PAKE protocol in the standard model

图 1 标准模型下高效的三方口令协议

2.2 安全性证明

本节给出我们所设计的三方 PAKE 协议的语义安全性的证明.

定理 1. 假设 \mathcal{A} 是一个运行时间为 t , 并且进行了 q_{send} 次主动攻击的概率多项式敌手. 假设 DDH 假设在循环群 G_q 中成立, 协议中所使用的对称加密算法满足对于单次加密的 CPA 安全性, 并且公钥加密算法 E 是 CCA 安全的, 那么敌手 \mathcal{A} 攻击本文的三方 PAKE 协议的语义安全的优势至多为

$$Adv_{\mathcal{P}, \mathcal{D}}^{ake-fs}(\mathcal{A}) \leq \frac{q_{send}}{|\mathcal{D}|} + neg(n),$$

其中, $neg(n)$ 表示关于安全参数 n 的一个可忽略函数.

证明: 本定理的证明由一系列混合实验组成: 第 1 个实验从真实的攻击游戏开始, 然后逐步对攻击游戏中的模拟规则进行修改, 并估计两个相邻实验之间敌手优势差距的上界, 直到敌手的攻击优势为 0 的实验结束. 我们首先修改被动攻击的模拟规则, 使得被动攻击中不泄露任何口令信息并且会话密钥完全随机, 然后逐步修改主动攻击中的模拟规则, 使得只有敌手正确猜测口令的条件下才有可能赢得攻击游戏. 我们用 $Adv(\mathcal{A}, P_i)$ 表示敌手 \mathcal{A} 在第 i 个混合实验中的优势.

实验 P_0 : 这个实验模拟了攻击游戏在标准模型下的真实运行. 根据敌手优势的定义有:

$$Adv_{\mathcal{P}, \mathcal{D}}^{ake-fs}(\mathcal{A}) = Adv(\mathcal{A}, P_0).$$

实验 P_1 : 从这个实验开始, 我们开始修改对敌手进行的被动攻击 *Execute* 询问的模拟规则. 对于敌手 \mathcal{A} 进行的 $Execute(A^i, S^j, B^k)$ 询问, 我们令用户 A 正常计算 $X_1 = g^x$, 但是在计算 X_2 时, 使用在口令空间之外随机选择的一个虚假口令 pw_A^* , 即, $X_2 = h^x g^{pw_A^*}$. 类似地, 用户 B 也用虚假口令 pw_B^* 计算 $Y_2 = h^y g^{pw_B^*}$. 服务器 S 在模拟时直接令 $X'_2 = h^x$ 和 $Y'_2 = h^y$, 并计算 $\sigma_A = X_1^i h^{x^2}$ 和 $\sigma_B = Y_1^i h^{y^2}$. 其余的模拟规则与真实的攻击游戏完全相同. 显然, 如果存在敌手能够以不可忽略的概率区分实验 P_1 和实验 P_0 , 那么我们可以构造算法以相同的优势攻破 ElGamal 加密算法的 CPA 安全性. 这个规约非常直观, 因此这里不再赘述. 由 ElGamal 加密算法的 CPA 安全性, 我们有:

$$|Adv(\mathcal{A}, P_1) - Adv(\mathcal{A}, P_0)| \leq neg(n).$$

实验 P_2 : 在这个实验中, 我们继续修改对敌手进行的 *Execute* 询问的模拟规则. 对于敌手 \mathcal{A} 进行的 $Execute(A^i, S^j, B^k)$ 询问, 我们在实验 P_1 修改的基础上进一步从循环群 G_q 中随机选择 σ_A 和 σ_B 的值. 由于在实验 P_1 中, 对于 *Execute* 询问的模拟使用的是虚假的口令, 因此由基于 ElGamal 加密算法的平滑投射哈希函数的平滑性保证了 σ_A 和 σ_B 的分布与 G_q 上的均匀分布是统计不可区分的. 根据平滑投射哈希函数的平滑性, 敌手区分实验 P_1 和实验 P_2 的优势是可忽略的. 我们有:

$$|Adv(\mathcal{A}, P_2) - Adv(\mathcal{A}, P_1)| \leq neg(n).$$

实验 P_3 : 在这个实验中, 我们继续修改对敌手进行的 *Execute* 询问的模拟规则. 对于敌手 \mathcal{A} 进行的 $Execute(A^i, S^j, B^k)$ 询问, 我们令服务器 S 随机选择适当长度的 $r_A || \tau_{A1} || \tau_{A2}$ 和 $r_B || \tau_{B1} || \tau_{B2}$, 而不是通过通用哈希函数簇计算. 相应地, 我们令用户端的相应值与 $r_A || \tau_{A1} || \tau_{A2}$ 和 $r_B || \tau_{B1} || \tau_{B2}$ 一致. 由通用哈希函数簇的性质可知: 当其输入为 G_q 中的随机值时, 通用哈希函数簇的输出与其值域中的均匀分布式统计不可区分的, 因此有:

$$|Adv(\mathcal{A}, P_3) - Adv(\mathcal{A}, P_2)| \leq neg(n).$$

实验 P_4 : 在这个实验中, 我们继续修改对敌手进行的 *Execute* 询问的模拟规则. 对于敌手 \mathcal{A} 进行的 $Execute(A^i, S^j, B^k)$ 询问, 我们进一步令服务器在计算 CCA 加密算法 E 的密文 ω_A 和 ω_B 时, 将输入中的 X'_2 和 Y'_2 用 G_q 中的两个随机值来替代. 由于在实验 P_3 中, 我们随机选择了加密时所用的随机输入 r_A 和 r_B , 因此, 实验 P_4 和上一个实验的差别至多是敌手攻破加密算法 E 的 CCA 安全的优势. 其实, 这里仅用到 CCA 加密算法 E 的 CPA 安全性. 与实验 P_1 的分析类似, 我们有:

$$|Adv(\mathcal{A}, P_4) - Adv(\mathcal{A}, P_3)| \leq neg(n).$$

实验 P_5 : 在这个实验中, 我们最后一次修改对敌手进行的 *Execute* 询问的模拟规则. 首先, 在产生公共参数中的 h 时, 我们随机选择 $s \in Z_q^*$ 并令 $h = g^s$. 此外, 对于敌手 \mathcal{A} 进行的 $Execute(A^i, S^j, B^k)$ 询问, 我们选择 G_q 中的一个随

机值作为会话密钥,而不是通过 $K = Y_1^{*x}$ 或者 $K = X_1^{*y}$ 来计算.实验 P_5 和上一个实验的差距至多是敌手攻破 DDH 假设的优势.给定一个 DDH 实例 (U, V, W) ,我们利用 DH 问题的自归约性来证明上述结论.为了模拟 $Execute(A^h, S^j, B^2)$ 询问,我们首先随机选择 $a_1, a_2, b_1, b_2 \in \mathbb{Z}_q^*$, 然后令 $X_1 = U^{a_1} g^{a_2}$ 以及 $Y_1 = U^{b_1} g^{b_2}$. 由于我们令 $h = g^s$, 因此可以按照实验 P_4 的规则正常模拟 $Execute$ 询问的剩余步骤.最后计算会话密钥的时候,定义会话密钥 $K = (W^{a_1 b_1} \cdot U^{a_1 b_2} \cdot V^{a_2 b_1} \cdot g^{a_2 b_2})^s$. 显然,如果 $W = CDH(U, V)$, 那么上述模拟与实验 P_4 完全一致;如果 $W \neq CDH(U, V)$, 那么上述模拟与实验 P_5 一致.如果存在敌手可以以不可忽略的优势区分实验 P_4 和 P_5 , 那么我们可以以同样的优势攻破 DDH 假设.我们有:

$$|Adv(\mathcal{A}, P_5) - Adv(\mathcal{A}, P_4)| \leq neg(n).$$

从实验 P_5 中,我们已经完成了对 $Execute$ 询问的模拟规则的修改.敌手不能通过 $Execute$ 询问获得用户口令的任何信息,因为在 $Execute$ 询问的模拟中我们使用了虚假的无效口令,因此在 $Execute$ 询问的会话模拟中不包含真实口令的任何信息;此外,由于 $Execute$ 询问的会话密钥是随机选择的,因此敌手通过 $Execute$ 询问进行攻击的优势是可忽略的.从下一个实验开始,我们对敌手进行的主动攻击的模拟规则进行修改.

在下一个实验开始之前,我们先进行一些预备工作.如果一条消息是诚实的参与者生成的,即使敌手转发了该消息,依然称该消息是实例产生的;否则,称该消息是敌手产生的.我们用 $Send_0(A, B, S)$ 表示敌手要求用户开始执行协议的初始激活消息;用 $SendClient_i(U, m)$ 表示敌手在某个会话的第 i 轮通信中冒充服务器给用户 U 发送消息 m , 用 $SendServer_i(S, m)$ 表示敌手在某个会话的第 i 轮通信中冒充用户给用户 S 发送消息 m . 在产生公开参数时,除了令 $h = g^s$ 外,我们还在产生公开参数中加密算法 E 的公钥 pk 的同时,记录其对应的私钥 sk .

实验 P_6 : 从这个实验开始,我们对敌手进行的主动攻击 $Send$ 询问的模拟规则进行修改.对于敌手伪造服务器的消息并对诚实用户 A (对于用户 B 的模拟类似) 进行的 $SendClient_2(A^h, C_A \parallel \mu \parallel \omega_A)$ 询问,假设 (A, X_1, X_2) 是用户 A 上一轮通信中对应于 $Send_0(A^h, B^2, S^j)$ 的回答,我们直接用密钥 sk 对 ω_A 解密,并验证解密得到的消息是否等于 $H(X_1, X_2', C_A, \mu, A, B, S)$, 其中, $X_2' = X_2 g^{-pw_A}$. 如果上述验证通过,则认为敌手攻击成功并结束攻击游戏的模拟;如果验证不通过,则拒绝该消息并停止对用户实例 A^h 的模拟.注意:对于敌手简单重放而没有进行修改的消息,这里的模拟规则与实验 P_5 相同.实验 P_6 和 P_5 相比,只是增加了敌手成功的一种方式,因此,敌手在实验 P_6 的优势将会增加.我们有:

$$|Adv(\mathcal{A}, P_6) - Adv(\mathcal{A}, P_5)| \leq neg(n).$$

实验 P_7 : 在这个实验中,我们对敌手进行的 $Send_0(A^h, B^2, S^j)$ 询问的模拟进行修改.对于未被腐化的用户 A (或 B) 接收到 $Send_0(A^h, B^2, S^j)$ 后,类似于实验 P_1 , 我们在计算消息 (A, X_1, X_2) (或消息 (B, Y_1, Y_2)) 时采用虚假的口令 pw_A^* (或 pw_B^*). 为了保证模拟的一致性,如果敌手在 $SendClient_2(A^h, C_A \parallel \mu \parallel \omega_A)$ 的询问中只是简单转发了服务器产生的消息,那么我们令用户 A 将服务器在模拟时产生的 $r_A \parallel \tau_{A1} \parallel \tau_{A2}$ 作为自己通用哈希函数的输出;否则类似于实验 P_6 , 我们对消息中密文 ω_A 进行解密来判断敌手是否成功.实验 P_7 和 P_6 的差别和敌手攻破 DDH 假设的优势相等.与实验 P_1 的分析类似,我们有:

$$|Adv(\mathcal{A}, P_7) - Adv(\mathcal{A}, P_6)| \leq neg(n).$$

实验 P_8 : 在这个实验中,我们对敌手冒充诚实用户 A 进行的 $SendServer_1(S^j, A \parallel X_1 \parallel X_2)$ 询问的模拟进行修改(敌手冒充诚实用户 B 的模拟类似).我们直接利用 h 对应于 g 的离散对数 s 对 X_2 进行解密,如果解密得到正确的口令,那么结束整个攻击游戏,得模拟并认为敌手成功.与实验 P_6 类似,敌手在这个实验里面只是增加了一种赢得攻击游戏的方式,因此敌手的优势将增加:

$$|Adv(\mathcal{A}, P_8) - Adv(\mathcal{A}, P_7)| \leq neg(n).$$

实验 P_9 : 在这个实验中,我们对敌手冒充诚实用户 A 进行的 $SendServer_1(S^j, A \parallel X_1 \parallel X_2)$ 询问的模拟继续进行修改(敌手冒充诚实用户 B 的模拟类似).我们利用 s 对 X_2 进行解密后,如果得到正确的口令,则认为敌手赢得了攻击游戏;如果解密得到的不是正确的口令,那么从循环群 G_q 中随机选择 σ_A 的值.由于敌手对于诚实用户 A 的口令猜测错误,因此根据平滑投射哈希函数的平滑性,有:

$$|Adv(\mathcal{A}, P_9) - Adv(\mathcal{A}, P_8)| \leq neg(n).$$

实验 P_{10} : 在这个实验中, 我们对敌手冒充诚实用户 A 进行的 $SendServer_1(S^j, A || X_1 || X_2)$ 询问的模拟继续进行修
改(敌手冒充诚实用户 B 的模拟类似). 我们利用 s 对 X_2 进行解密后, 如果得到正确的口令, 则认为敌手赢得攻击
游戏; 否则在实验 P_9 的模拟规则的基础上, 进一步随机选择 $r_A || \tau_{A1} || \tau_{A2}$. 由通用哈希函数簇的性质可知: 当输入为
 G_q 的随机值的时候, 通用哈希函数簇的输出与其值域中的均匀分布是统计不可区分的. 因此, 我们有:

$$|Adv(\mathcal{A}, P_{10}) - Adv(\mathcal{A}, P_9)| \leq neg(n).$$

实验 P_{11} : 在这个实验中, 我们对敌手冒充诚实用户 A 进行的 $SendServer_1(S^j, A || X_1 || X_2)$ 询问的模拟最后一次进
行修改(敌手冒充诚实用户 B 的模拟类似). 在实验 P_{10} 模拟规则的基础上, 我们在在计算 CCA 加密算法的密文
 ω_A 时, 采用在 G_q 中随机选择的值来替代 X_2' , 从而保证在敌手没有猜测到正确口令的主动攻击中得不到关于用
户口令的任何信息. 实验 P_{11} 与实验 P_{10} 的差别至多是敌手攻破公钥加密算法 E 的 CCA 安全的优势.

与实验 P_4 的分析类似, 但是这里我们需要用到公钥加密算法 E 的 CCA 安全性. 原因在于: 根据我们对敌手
进行的 $SendClient_2(A^h, C_A || \mu || \omega_A)$ 的模拟规则, 需要利用 CCA 攻击游戏中的解密谕示帮助我们解密消息中密
文 ω_A , 从而判断敌手是否成功. 根据公钥加密算法 E 的 CCA 安全性, 我们有:

$$|Adv(\mathcal{A}, P_{11}) - Adv(\mathcal{A}, P_{10})| \leq neg(n).$$

实验 P_{12} : 在这个实验中, 我们对敌手冒充诚实用户 A 进行的 $SendServer_3(S^j, A || \tau'_{A2})$ 询问的模拟进行修改(敌
手冒充诚实用户 B 的模拟类似). 如果敌手伪造的 τ'_{A2} 与我们随机选择的 τ_{A2} 相等, 那么我们认为敌手成功.

显然, 如果敌手在 $SendServer_1(S^j, A || X_1 || X_2)$ 在猜测到正确的口令, 我们已经令敌手获胜; 如果敌手发送
 $SendServer_3(S^j, A || \tau'_{A2})$, 说明敌手在第 1 轮消息中没有猜到正确的口令. 根据模拟规则, 我们将从值域中随机选
择 $r_A || \tau_{A1} || \tau_{A2}$, 因此, 敌手正确猜测到 τ_{A2} 的概率是可忽略的. 我们有:

$$|Adv(\mathcal{A}, P_{12}) - Adv(\mathcal{A}, P_{11})| \leq neg(n).$$

实验 P_{13} : 在这个实验中, 我们最后一次对敌手冒充诚实用户 A 进行的 $Send$ 询问的模拟进行修改. 如果敌手
没有发送 $SendServer_3(S^j, A || \tau'_{A2})$, 但是敌手从服务器在第 2 轮发送的消息 (S, C_A, μ, ω_A) 利用对称加密算法的密文
 C_A 得到了 Y_1^* , 那么我们认为敌手成功. 显然, 在这个实验里面, 敌手多了一种获胜的方式. 但是, 由于我们所使用
的对称加密对于单次加密是 CPA 安全的, 而我们随机选择通用哈希函数簇的输出, 因此随机选择的输出(即对称
加密算法的密钥)发生碰撞的概率是可忽略的. 根据对称加密的 CPA 安全性, 我们有:

$$|Adv(\mathcal{A}, P_{13}) - Adv(\mathcal{A}, P_{12})| \leq neg(n).$$

现在我们来分析敌手在这个实验里面赢得攻击游戏的几种方式:

- 方式 1: 对于敌手产生的 $SendServer_1(S^j, A || X_1 || X_2)$ 询问(对于敌手冒充用户 B 的模拟类似), 如果对 X_2 解密
后发现敌手猜测口令正确, 则认为敌手赢得攻击游戏;
- 方式 2: 对于敌手伪造服务器的消息并对诚实用户 A 进行的 $SendClient_2(A^h, C_A || \mu || \omega_A)$ 询问(对于敌手
冒充用户 B 的模拟类似), 如果对密文 ω_A 解密后发现该密文包含了正确的口令信息, 则认为敌手赢得攻
击游戏;
- 方式 3: 敌手在没有正确猜测到口令的条件下, 通过 $SendServer_3(S^j, A || \tau'_{A2})$ 询问正确猜测到了 τ_{A2} 的值,
同样认为敌手获胜;
- 方式 4: 敌手没有通过上述的 3 种方式获胜, 但是从密文 C_A 中得到了 Y_1^* , 那么我们认为敌手获胜;
- 方式 5: 敌手成功猜测到 $Test$ 询问中所使用的随机比特.

显然, 敌手通过方式 3 和方式 4 获胜的概率是可忽略的. 我们用 $PwGuess$ 表示事件敌手通过方式 1 或方式 2
正确猜测到口令; 用 $Success$ 表示事件敌手通过方式 5 猜测到 $Test$ 询问中所使用的随机比特而获胜. 由于我们在
模拟协议运行时, 在敌手没有猜测到正确口令的条件下不会在模拟中用到任何口令的信息, 因此有:

$$Pr[PwGuess] \leq \frac{q_{send}}{|\mathcal{D}|}.$$

如果事件 $PwGuess$ 不发生,那么由于敌手通过方式 3 和方式 4 获胜的概率是可忽略的,因此敌手只能通过方式 5 赢得攻击游戏.但是,由于在敌手进行的主动攻击中,诚实用户的实例由于敌手在第 2 轮无法产生正确的消息 (S, C_A, μ, ω_A) 从而拒绝接受;而在被动的会话中,所有的会话密钥是随机选择的,因此敌手通过方式 5 成功的概率是 $\frac{1}{2}$.忽略方式 3 和方式 4,我们有:

$$\begin{aligned} \Pr[Success] &= \Pr[Success \wedge PwGuess] + \Pr[Success \wedge \overline{PwGuess}] \\ &\leq \Pr[PwGuess] + \Pr[Success | \overline{PwGuess}] \cdot (1 - \Pr[PwGuess]) \\ &= \frac{1}{2} + \frac{1}{2} \cdot \Pr[PwGuess] \\ &\leq \frac{1}{2} + \frac{1}{2} \cdot \frac{q_{send}}{|\mathcal{D}|}. \end{aligned}$$

综合上面所有的等式结果,定理 1 得证. □

定理 2. 假设 \mathcal{A}_{kp} 是一个运行时间为 t 并且进行了 $q_{execute}$ 次被动攻击的概率多项式敌手.假设 DDH 假设在循环群 G_q 中成立,那么敌手 \mathcal{A}_{kp} 攻击本文的三方 PAKE 协议的密钥私密性的优势至多为

$$Adv_{\mathcal{P}, \mathcal{D}}^{ake-kp}(\mathcal{A}) \leq q_{execute} Adv_{G_q}^{DDH}(O(t)),$$

其中, $Adv_{G_q}^{DDH}(O(t))$ 表示在多项式时间内破解 DDH 假设的优势.

证明:假设 \mathcal{A}_{kp} 是一个运行时间为 t 并且进行了 $q_{execute}$ 次被动攻击的概率多项式敌手.如果 \mathcal{A}_{kp} 可以破坏协议的密钥私密性,那么我们可以通过敌手 \mathcal{A}_{kp} 的能力来解决 DDH 问题.

给定 DDH 问题的一个实例 (U, V, W) ,我们首先根据口令空间 \mathcal{D} 的分布为所有用户选择口令并相应的选择所有的公共参数,并且将所有用户的口令告诉敌手 \mathcal{A}_{kp} .在攻击游戏模拟阶段,我们令模拟者随机猜测 $q_{execute}$ 次被动攻击中的一次会话作为敌手 \mathcal{A}_{kp} 的测试会话,对于其余的会话都正常模拟.显然,猜测正确测试会话的概率为 $1/q_{execute}$.对于猜测的测试会话,我们令 $X_1=U, Y_1=V$,并且随机令服务器选择 z ,计算 $X_1^* = X_1^z, Y_1^* = Y_1^z$.其余的模拟按照协议的描述执行.如果 \mathcal{A}_{kp} 没有选择预先选定的会话作为测试会话,则跳出本次攻击游戏的模拟;否则,当敌手 \mathcal{A}_{kp} 对测试会话进行 $TestPair$ 询问时,我们返回 $K=W^z$ 作为回答.显然:如果 (U, V, W) 是 Diffie-Hellman 三元组,那么返回的是真实的会话密钥;否则,返回的是一个与会话密钥等长的随机数.此时,敌手 \mathcal{A}_{kp} 赢得攻击游戏的优势等同于解决 DDH 假设的优势.由于模拟者猜测正确测试会话的概率为 $1/q_{execute}$,因此定理得证. □

3 协议性能比较

在本节,我们对本文的协议和已有的标准模型下的三方口令认证密钥交换协议^[20-22]从效率和安全性两个方面进行比较.

在计算代价方面,我们主要考虑计算代价较高的模幂运算(用 e 表示)和公钥加解密运算,而忽略其余的运算(诸如哈希函数、对称加密和 MAC 等).我们采用标准模型下 CCA 安全的 DHIES 公钥加密算法来对参与比较的协议中所使用的 CCA 安全的加密体制进行实例化^[24],从而将公钥加解密的计算代价转化为模幂运算的个数. DHIES 算法加密时需要两个模幂运算,解密时需要一个模幂运算.由于形如 $g^x h^y$ 的两个模幂运算的乘积可以通过一个模幂运算的代价求得,因此对于此类运算,我们只计为一个模幂运算.在通信代价方面,三方口令认证密钥交换协议多用于无线通信环境,而在无线环境下,协议的交互轮数远比通信带宽重要,因此我们主要考虑协议的执行轮数.由于文献[22]采用了模块化的设计思路,通过安全的两方 PAKE 协议来构造三方 PAKE 协议,因此我们用目前标准模型下效率最高的 Jiang 等人的两方 PAKE 协议^[5]对该协议进行实例化.在安全性方面,由于参与比较的协议都提供了相同的安全属性,因此我们主要从服务器是否具有公钥证书和证明所基于的困难性假设来进行比较,其中,ODH 代表 DHIES 算法的安全性所基于的 Oracle Diffie-Hellman 假设.

从表 1 可以看出:我们的协议在计算代价方面低于 NRK 协议^[22],与 YC 协议^[21]的计算代价相当,而计算代价高于 KJL 协议^[20],但是我们的协议在通信轮数方面要明显低于 NRK 协议.虽然 NRK 协议可以通过标准模型

下一轮的 PAKE 进行实例化从而降低轮数,但是目前,标准模型下最高效的一轮的 PAKE 中,每个参与者需要至少 12 个模幂运算^[25],这将会极大增加协议的计算代价.KJL 协议虽然只需要两轮通信,并且计算效率高于我们的协议,但是该协议假设服务器拥有公钥证书,并不是完全基于口令认证的;并且,用户需要知道服务器的公钥,这将给用户的使用带来不便.

Table 1 Cost comparison with existing protocols for 3PAKE in the standard model

表 1 标准模型下三方口令协议的性能比较

| 比较的协议 | 通信轮数 | 计算代价 | | | 服务器公钥证书 | 困难性假设 |
|------------------------|------|------|-----|-----|---------|----------|
| | | 用户 | 服务器 | 总代价 | | |
| KJL 协议 ^[20] | 2 | 4e | 2e | 10e | 是 | DDH, ODH |
| YC 协议 ^[21] | 3 | 5e | 8e | 18e | 是 | DDH |
| NRK 协议 ^[22] | 6 | 9e | 12e | 30e | 否 | DDH |
| 我们的协议 | 3 | 6e | 9e | 21e | 否 | DDH,ODH |

4 结束语

本文以基于 ElGamal 加密的平滑投射哈希函数为工具设计了一种安全高效的三方 PAKE 协议,并且在标准模型下,基于 DDH 假设证明了其安全性.我们的协议实现了用户和服务器之间的双向认证并且具有前向安全性.与同类的协议相比,新协议完全基于口令实现用户认证,并且具有较高的通信和计算效率.因此,我们的协议更适用于大规模端到端通信的应用环境.

References:

- [1] Bellare SM, Merritt M. Encrypted key exchange: Password-Based protocols secure against dictionary attacks. In: Proc. of the IEEE Symp. on Research in Security and Privacy. Los Alamitos: IEEE Computer Society, 1992. 72–84. [doi: 10.1109/RISP.1992.213269]
- [2] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attack. In: Preneel B, ed. Proc. of the EUROCRYPT 2000. LNCS 1807, Berlin: Springer-Verlag, 2000. 140–156. [doi: 10.1007/3-540-45539-6_11]
- [3] Boyko V, MacKenzie P, Patel S. Provably secure password-authenticated key exchange using Diffie-Hellman. In: Preneel B, ed. Proc. of the EUROCRYPT 2000. LNCS 1807, Berlin: Springer-Verlag, 2000. 156–171. [doi: 10.1007/3-540-45539-6_12]
- [4] Katz J, Ostrovsky R, Yung M. Efficient password-authenticated key exchange using human-memorable passwords. In: Pfitzmann B, ed. Proc. of the EUROCRYPT 2001. LNCS 2045, Berlin: Springer-Verlag, 2001. 475–494. [doi: 10.1007/3-540-44987-6_29]
- [5] Jiang SQ, Gong G. Password based key exchange with mutual authentication. In: Handschuh H, Hasan A, eds. Proc. of the SAC 2004. LNCS 3357, Berlin: Springer-Verlag, 2004. 267–279. [doi: 10.1007/978-3-540-30564-4_19]
- [6] Canetti R, Halevi S, Katz J, Lindell Y, MacKenzie P. Universally composable password-based key exchange. In: Cramer R, ed. Proc. of the EUROCRYPT 2005. LNCS 3494, Berlin: Springer-Verlag, 2005. 404–421. [doi: 10.1007/11426639_24]
- [7] Lin CL, Sun HM, Hwang T. Three-Party encrypted key exchange: Attacks and a solution. ACM SIGOPS Operation System Review, 2000,34(4):12–20. [doi: 10.1145/506106.506108]
- [8] Lin CL, Sun HM, Steiner M, Hwang T. Three-Party encrypted key exchange without server public-keys. IEEE Communications Letters, 2000,5(12):497–499. [doi: 10.1109/4234.974498]
- [9] Abdalla M, Fouque PA, Pointcheval D. Password-Based authenticated key exchange in the three-party setting. In: Vaudenay S, ed. Proc. of the PKC 2005. LNCS 3386, Berlin: Springer-Verlag, 2005. 65–84. [doi: 10.1007/978-3-540-30580-4_6]
- [10] Abdalla M, Pointcheval D. Interactive Diffie-Hellman assumptions with applications to password-based authentication. In: Patrick AS, ed. Proc. of the FC 2005. LNCS 3570, Berlin: Springer-Verlag, 2005. 341–356. [doi: 10.1007/11507840_31]
- [11] Wang WJ, Hu L. Efficient and provably secure generic construction of three-party password-based authenticated key exchange protocols. In: Barua R, ed. Proc. of the INDOCRYPT 2006. LNCS 4329, Berlin: Springer-Verlag, 2006. 118–132. [doi: 10.1007/11941378_10]
- [12] Yoneyama K. Efficient and strongly secure password-based server aided key exchange. In: Chowdhury DR, ed. Proc. of the INDOCRYPT 2008. LNCS 5365, Berlin: Springer-Verlag, 2008. 172–184. [doi: 10.1007/978-3-540-89754-5_14]

- [13] Zhao JJ, Gu DW. Provably secure three-party password-based authenticated key exchange protocol. *Information Sciences*, 2012, 184(1):310–323. [doi: 10.1016/j.ins.2011.07.015]
- [14] Huang HF. A simple three-party password-based key exchange protocol. *Int'l Journal of Communication Systems*, 2009, 22(7): 857–862. [doi: 10.1002/dac.1002]
- [15] Yoon EJ, Yoo KY. Cryptanalysis of a simple three-party password-based key exchange protocol. *Int'l Journal of Communication Systems*, 2011,24(4):532–542. [doi: 10.1002/dac.1168]
- [16] Wu SH, Chen KF, Zhu YF. Enhancements of a three-party password-based authenticated key exchange protocol. *Int'l Arab Journal of Information Technology*, 2013,10(3):215–221.
- [17] Lee TF, Hwang T. Simple password-based three party authenticated key exchange without server public keys. *Information Sciences*, 2010,180(9):1702–1714. [doi: 10.1016/j.ins.2010.01.005]
- [18] Chang TY, Hwang MS, Yang WP. A communication-efficient three party password authenticated key exchange protocol. *Information Sciences*, 2011,181(1):217–226. [doi: 10.1016/j.ins.2010.08.032]
- [19] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited. *Journal of the ACM*, 2004,51(4):557–594. [doi: 10.1145/1008731.1008734]
- [20] Kwon JO, Jeong IR, Lee DH. Light-Weight key exchange with different passwords in the standard model. *Journal of Universal Computer Science*, 2009,15(5):1042–1064. [doi: 10.3217/jucs-015-05-1042]
- [21] Yang JH, Cao TJ. Provably secure three-party password authenticated key exchange protocol in the standard model. *The Journal of Systems and Software*, 2012,85:340–350. [doi: 10.1016/j.jss.2011.08.024]
- [22] Nam JH, Raymond Choo KK, Kim J, Paik J, Won D. Password-Only authenticated three-party key exchange with provable security in the standard model. *The Scientific World Journal*, 2014, Article ID 825072. [doi: 10.1155/2014/825072]
- [23] Cramer R, Shoup V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public key encryption. In: Kundsén LR, ed. *Proc. of the EUROCRYPT 2002*. LNCS 2332, Berlin: Springer-Verlag, 2002. 45–64. [doi: 10.1007/3-540-46035-7_4]
- [24] Abdalla M, Bellare M, Rogaway P. The oracle Diffie-Hellman assumptions and an analysis of DHIES. In: David N, ed. *Proc. of the CT-RSA 2001*. LNCS 2020, Berlin: Springer-Verlag, 2001. 143–158. [doi: 10.1007/3-540-45353-9_12]
- [25] Benhamouda F, Blazy O, Chevalier C, Pointcheval D, Vergnaud D. New techniques for SPHF and efficient one-round PAKE protocols. In: Canetti R, ed. *Proc. of the CRYPTO 2013*. LNCS 8042, Berlin: Springer-Verlag, 2013. 449–475. [doi: 10.1007/978-3-642-40041-4_25]



魏福山(1983—),男,甘肃武威人,博士,讲师,主要研究领域为安全协议,无线网络安全认证.



李光松(1977—),男,博士,副教授,主要研究领域为无线网络安全.



马建峰(1963—),男,博士,教授,博士生导师,主要研究领域为计算机系统安全,移动/无线安全,系统可生存性,可信计算.



马传贵(1962—),男,博士,教授,博士生导师,主要研究领域为信息安全.