计算机学报'11 基于RSA的网关口令认证密钥交换协议

基于PEKEP协议，提出了基于RSA的可证明安全的网关口令认证密钥交换协议，在Rom下，基于RSA假设证明了协议的安全性，可抵抗e次剩余攻击和不可检测在线字典攻击.

优点：①基于PEKEP提出了基于RSA的GPAKE，在用户端和网关端的计算效率较高，符合实际需求 ②在Rom下证明了语义安全性及密钥私密性，证明过程较清晰 ③协议介绍较清晰

问题：①引言部分提到了GPAKE的安全目标，但漏掉了AKE的认证性，且下文分析中也未提及 ②在形式化证明中，对于口令保护未给出证明，而是认为PEKEP的结论可带来这个结论，但本文G与S的交互过程并非与PEKEP一致，gcd(α,n)≠1时并非终止会话，而是选择随机数，而前者会泄露信息. ③1.2中提到匿名性会导致不能抵抗不可检测字典攻击，未解释原因 ④图片(流程图)不清楚，符号可在介绍协议前统一说明.

GPAKE的介绍

目标：用户C ↔(建立sk，不安全通道)↔ 网关G ↔(安全通道)↔ 服务器S. 共享pw.

如果服务器可以做主动攻击呢？

文中定义的3个安全目标(缺少认证性).

1) sk的语义安全性，通过 Real-or-Random(ROR)攻击游戏模型化

2) 密钥私密性：服务器无法得知 C、G之间的会话密钥 ←降低对S的信任(CA不可做主动攻击).

3) 口令保护：网关不可从服务器处获得用户口令的信息.

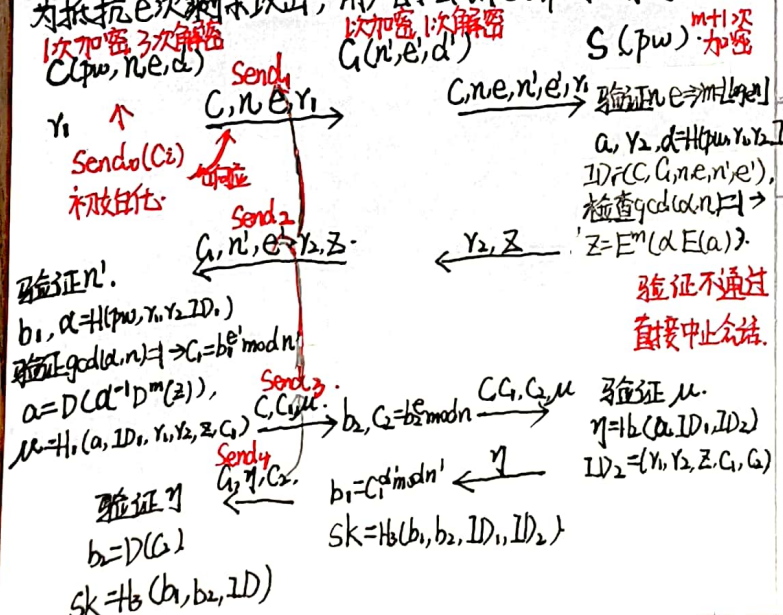
3个参与者：U=C∪G∪S，U持有口令，S持有对应口令列表.

除了Execute、Send和Test，为了满足密钥私密性，先前文献引入了Test Pair查询，输入为两个实例，输出为共享的sk或随机值.

▲密钥私密性：敌手A已知所有口令，但不可做主动攻击，无法区分sk和随机值，则满足sk私密性.

基于RSA的GPAKE协议(基于PEKEP完成设计). 4轮交互.

为抵抗e次剩余攻击，用户的公钥e取为奇素数次.



语义安全性证明 5个实验 $P_0 \sim P_4$，$Adv(A, P_i)$表示A在第i个实验的优势. $H: \{0,1\}^* \to Z_n$，$H_{1\sim3}: \{0,1\}^* \to \{0,1\}^k$

P_0 真实的攻击，可估次Send、Execute、Test询问，另外H、$H_{1\sim3}$都维护一个输入输出的列表. $\Rightarrow Adv(A)=Adv(A, P_0)$

P_1：修改对Execute询问的模拟，sk不通过H_3计算得到，而是从$\{0,1\}^k$中取随机数代替

敌手区分P_0和P_1，即破解RSA问题.

P_0中，sk从H_3得到，$sk=H_3(b_1, b_2, ID)$，敌手若不知b_1、b_2则无法区分sk和随机数(假设敌手只需得到b_2，概率Pb_2)

$\Rightarrow$ 定义1个游戏：$|Adv(A,P_1)-Adv(A,P_0)| \le (q_{Execute}(Adv^{rsa}(Ot) + \frac{q_{oh}}{\varphi(n)})$.

G_1：敌手A诚实运行 C^i和G^j，且最后输出b_2的猜测

G_2：与G_1类似，但计算μ和η时用私有的随机预言

易得 $Pb_2=Pb_2(G_1)$，$Ask H_{1,2}$表示敌手询问了H_1或H_2. 次数q_{oh}

则有 $|Pb_2(G_1)-Pb_2(G_2)| \le Pr[Ask H_{1,2}]$

有：$Pr[Ask H_{1,2}]=\frac{q_{oh}}{\varphi(n)}$，$Pb_2=Pb_2(G_1) \le Pb_2(G_2)+\frac{q_{oh}}{\varphi(n)}$

对于G_2，需设计算法C解密 c，则C对应的明文为解

有 $Pb_2(G_2) \le Adv^{rsa}(Ot))$，$Pb_2 \le Adv^{rsa}(Ot)) + \frac{q_{oh}}{\varphi(n)}$

(主动攻击在图中给出标号，消息由实例产生$\Rightarrow$预言生成，否则为敌手产生).

P_2：G^j在$Send_1$收到C^i按协议生成的(C, n, e, Y_1)，若G^j、C^i诚实接受，则sk为随机值；若只有C诚实接受，则G^j会话密钥为随机值，C^i不定义sk.(同PEKEP).

由于私钥对敌手来说未知，故不可得a.有

$|Adv(A.P_2)-Adv(A.P_1)| \le q_{Send} Adv^{rsa}(O(t))$.

P_3：C^i在$Send_2$收到G^j的(n', e', Y_2, Z)，若G^j和C^i都诚实接受，则sk为随机值.

易知与P_2优势相同，$Adv(A, P_2)=Adv(A, P_3)$

P_4：若$C^i(G^j)$在$Send_2(Send_1)$中收到敌手的消息，若最终$C^i(G^j)$接受，则实验结束敌手胜利. $Adv(A, P_3) \le Adv(A, P_4)$.

q_{Send1}和q_{Send2}为敌手做$Send_{1(2)}$的次数.

1) C^i在$Send_2$中收到敌手消息，可返回敌手μ和C_1，敌手若成功，必须得到η，但敌手未知α，概率至多为$\frac{1}{|D|}$，P_a表示得到α的概率. 则：$Pr[Succ] \le \frac{q_{Send2}}{|D|} + P_a \cdot q_{Send2} \cdot Adv^{rsa}(O(t)) + \frac{q_{Send2} q_{oh}}{\varphi(n)} + \frac{q_{Send2}}{2^k}$

其中 $P_a \le Pr.(\lambda_i=\alpha)_{PEKEP} + Adv^{rsa}(O(t)) + \frac{q_{oh}}{\varphi(n)} \le \frac{1}{|D|} + Adv^{rsa}(O(t)) + \frac{q_{oh}}{\varphi(n)}$

2) G^j在$Send_1$中收到敌手消息，应返回(Y_2, Z)给敌手，敌手应返回μ同上，P_a为敌手获得α的概率. 由于敌手有(e,n)，故对于入，可解 $(\lambda X^e)^{em} = Z \bmod n$，若$X=\alpha$，则$\lambda=\alpha$，否则与e为奇素数次一假设矛盾，则有 $P_a=Pr[\lambda=\alpha]=\frac{1}{|D|}$， $Pr[Succ] \le \frac{q_{Send1}}{|D|} + \frac{q_{Send2}}{2^k}$

可知P_4成功的概率$\Rightarrow$ $Adv(A, P_4)=2Pr[Succ_4]-1$

代入回去可得 $Adv^{ake\text{-}ror}_{P,D}(A)$.

密钥私密性与上区别为敌手已知口令，但对区分sk和随机值无帮助

口令保护，文中证明同P_4 2).