2004 - ASIACRYPT - Muxiang Zhang

New Approaches to Password Authenticated key Exchange based on RSA

**总结**：在基于RSA的PAKE协议安全性普遍较弱，而安全的SNAPI协议要求e为大素数且>n故实用性较差的背景下，作者提出了PEKEP，该协议允许e为小素数且可抵抗e次剩余攻击。作者基于RSA假设和ROM模型进行形式化安全分析，并进一步提出了具有更高效率的CEKEP。这两种协议只需实体共享口令，和无需其它参数。

**安全模型**：定义实体A,B∈I，共享口令p，在协议Π中双向鉴别并生成会话密钥。$\Pi_A^i$表示实体A的第i个协议实例(instance/oracle)，已接受的实例拥有会话密钥sk，会话标识sid和伙伴标识pid。

▲敌手的能力：主动、被动字典攻击，还可从已接受的实例中获取sk。敌手可向协议实例发送预言查询，包括：（结合BPR2000文里解释，认为一些解释没有很清晰析，如Test）

① Send(A,i,m)：中间人攻击，敌手向$\Pi_A^i$发M，并接收回应

② Execute(A,i,B,j)：窃听攻击，获取$\Pi_A^i$与$\Pi_B^j$交互的信息

③ Reveal(A,i)：$\Pi_A^i$的sk发送给敌手。

④ Test(A,i)：标识sk的语义安全性，它生成随机比特位，若b=1则返回sk，b=0返回随机串。只能执行一次。

⑤ Oracle(M)：敌手可访问函数h，传值可相应求解。

▲协议实例新鲜度：①实例已接受 ②实例和伙伴都未被Reveal过。

▲敌手的攻击目标：Succ表示A向新鲜实例做Test并猜测b'=b

敌手A的优势为：$Adv_A^{ake}=2Pr(Succ)-1$

**安全的PAKE协议**：希望敌手一次只能测试一个口令。

以Send查询标识猜测的次数，每个实例只记录一次Send。则一个安全PAKE协议，指敌手至多做$q_{send}$(≤|D|)次Send查询，且满足以下两个条件：

① Execute查询一定是针对一对已接受的实例$\Pi_A^i$和$\Pi_B^j$进行的。

② $Adv_A^{ake}\le\frac{q_{send}}{|D|}+\varepsilon$，其中ε可忽略，|D|为口令空间，表明敌手的攻击能力只与它在线交互的次数有关

**PEKEP** 基于RSA的PAKE协议，允许使用小素数作为e

A,B∈I，口令w∈D，A生成n,e,d，n为大奇数，e为奇素数。条件$C_1$

哈希函数$H_0,H_1,H_2,H_3:\{0,1\}^*\to\{0,1\}^k$，$H:\{0,1\}^*\to Z_n$，k为安全参数。

▲流程（以下判断语句后均为条件成立，才执行，除特别说明）。

① A→B：$r_A\in_R\{0,1\}^k$，n,e,A.（开始为Send0）

B验证$C_1$，$m=\lfloor\log_e n\rfloor$，选$\alpha\in_R Z_n^*$，$r_B\in_R\{0,1\}^k$，$\delta=H(w,r_A,r_B,A,B,n,e)$

验证$gcd(\alpha,n)=1$，若成立$\lambda=\alpha$，否则$\lambda\in_R Z_n^*$，计算$Z=E^m(\lambda E(\alpha))$ （Send1，$D_1$）

② B→A：$r_B$，Z。（Send2）

A计算：$\alpha=H(w,D_1)$，验证$gcd(\alpha,n)=1$，不成立⇒$b\in_R Z_n$；

成立⇒$b=D(\alpha^{-1}D^m(Z))$，计算$\mu=H_1(b,D_1)$.

③ A→B：μ.（Send3）

B验证$\mu\overset{?}{=}H_1(\alpha,D_1)$，计算：$\eta=H_2(\alpha,D_1)$，$sk=H_3(\alpha,D_1)$

④ B→A：η.（Send4）

A验证：$\eta\overset{?}{=}H_2(b,D_1)$，计算$sk=H_3(b,D_1)$.

▲gcd(α,n)判时拒绝，但为了不泄露信息，会用随机数继续协议。当n=p·q且p,q足够大且size接近时，gcd(α,n)≠1概率很低

▲上述流程除检查e与φ(n)是否互素，若e|φ(n)，可能导致e次剩余攻击

**定理1**证明了PEKEP可抵抗e次剩余攻击。✓对数说知识也做了能招

因为敌手可猜测口令⇒α⇒验证$(\lambda x^e)^{e^m}\equiv z\pmod{n}$是否在$Z_n^*$上有解，若有则无法排除口令，无则可以排除口令，若都有解，则不可排除

对于$e^{m+1}\nmid\varphi(p_2^{q_2})$，若z是n的$e^m$次剩余，则证对于$\forall\lambda\in Z_n^*$，$(\lambda x^e)^{e^m}\equiv z\pmod n$在$Z_n^*$上有解。$n_2=p_2^{q_2}$，只需证：$(\lambda x^e)^{e^m}\equiv z\pmod{n_2}$

$\varphi(n_2)=p_2^{q_2-1}(p_2-1)$，$g^{\varphi(n_2)}=1\bmod n_2$，$gcd(e^m,\varphi(n_2))=e^c$，$0\le c\le m$

①当c=0时，e与φ(n)互素，$(\lambda x^e)^{e^m}\equiv z\pmod{n_2}$有唯一解。

②1≤c≤m时，z为n的$e^m$次剩余，证$y^{e^m}\equiv z\pmod{n_2}$在$Z_{n_2}^*$上有解⇒

$e^m ind_g y\equiv ind_g z\pmod{\varphi(n_2)}$，以$ind_g y$为变量，则在$Z_{n_2}^*$上有$e^c$个解。（数论）

代入$y_0$，$ind_g y=ind_g y_0+t\cdot\frac{\varphi(n_2)}{e^c}\bmod\varphi(n_2)$，$0\le t\le e^c-1$.

对任意$\lambda\in Z_n^*$，$ind_g y-ind_g\lambda\equiv ind_g y_0-ind_g\lambda+t\cdot\frac{\varphi(n_2)}{e^c}\pmod{\varphi(n_2)}$

由$e^{m+1}\nmid\varphi(n_2)\Rightarrow e\nmid\varphi(n_2)/e^c$，$gcd(e,\frac{\varphi(n_2)}{e^c})=1$，e有本元根$g_e$.

$g_e^{\frac{\varphi(n_2)}{e^c}}\bmod e\equiv\frac{\varphi(n_2)}{e^c}$，故$ind_g y_0-ind_g\lambda+t\cdot\frac{\varphi(n_2)}{e^c}\equiv 0\pmod e$成立

即：$ind_g y-ind_g\lambda=0\pmod e$成立，有$y\cdot\lambda^{-1}=g^{ke}\bmod n_2$.

故存在$y\in Z_n^*$，$y^{e^m}\equiv z\pmod{n_2}$，$y\cdot\lambda^{-1}$为e次剩余？$\equiv z\lambda^e\bmod n_2$

因此②在$Z_n^*$上有解，得证。（介绍过程存在笔误"It is clear"的结论可能并不直观）

在PEKEP中，$m=\lfloor\log_e n\rfloor$，$e^{m+1}>n\ge p_2^{q_2}$，故PEKEP符合定理1。

且，PEKEP允许B选小的e替换A的公钥，符合$gcd(e,\varphi(n))=1$，A也可换可减少SNAPI中素数测试的开销，允许用小素数，实用性好。✓

在协议中，B做m+1次加密，$m=\lfloor\log_e n\rfloor$，时间为$O((\log_2 n)^3)$，与SNAPI同

A已知φ(n)只需2次解密，（B的运算负载依然较大）。

**CEKEP**：减少了加密次数，少于$\lfloor\log_e n\rfloor$次。比PEKEP多了2个flow

B选择$\xi(\sim 2^{-80})$，A生成$\rho$，$r_A\in_R\{0,1\}^k$，B生成$m=\lfloor\log_e n\rfloor$，$\rho\in_R\{0,1\}^{|n|}$并计算：

$\gamma=H(n,e,\rho,B,A,B,m)$与n互素，发送B,m给A，A计算$\gamma$，$u=D^m(\gamma)$

B判断$\gamma\overset{?}{=}E^m(u)$来看A有无解密能力（后续与PEKEP同）

若正确，$\gamma=E^m(u)$，定理7证明$e^m|\varphi(p_2^{q_2})$的概率为$e^{-m}$即≤ξ（无法进行$e^m$次剩余攻击）

证：$n_2=p_2^{q_2}$，且有$e^m|\varphi(n_2)$，$n_2$有本原根g，$\forall\gamma\in_R Z_n^*$

则：若γ为n以上的$e^m$剩余⇔$x^{e^m}\equiv\gamma\pmod{n_2}$有解，⇔（根据1）

$e^m ind_g x\equiv ind_g\gamma\pmod{\varphi(n_2)}$又$e^m|\varphi(n_2)$，故⇔$e^m|ind_g\gamma$

令$n_{\bar2}=n/n_2$，$n_2$与$n_{\bar2}$互素，对$\alpha_1\in Z_{n_2}^*$，$\alpha_2\in Z_{n_{\bar2}}^*$，由中国剩余定理：

存在$\alpha\in Z_n^*$，$\alpha\equiv\alpha_1\pmod{n_2}$，$\alpha\equiv\alpha_2\pmod{n_{\bar2}}$

故满足$\alpha\equiv\alpha_1\pmod{n_2}$的α有$\varphi(n_2)$个，对于$0\le s\le\varphi(n_2)-1$，

$Pr(g^s\equiv\gamma\bmod n_2)=\frac{\varphi(n_2)}{\varphi(n_2)}=\frac{1}{\varphi(n_2)}\Rightarrow Pr(ind_g\gamma=s)=\frac{1}{\varphi(n_2)}$

故$Pr(e^m|ind_g\gamma)=\frac{e^m}{e^m s}=e^{-m}$，故得证，$e^m|\varphi(p_2^{q_2})$的概率

故可进行e次剩余攻击（$0\le s<\varphi(n_2)$）概率不超过ξ（仅证明了结论，但未说明为什么如此设计，有什么依据？）

▲性能角度CEKEP中B主要为$u^{e^m}\bmod n$与$(\lambda a^e)^{e^{m-1}}\bmod n$，计算时间为$O(2(\log_2\xi^{-1})(\log_2 n)^2)$.（计算时间的得来不清楚）

ξ决定了计算的时间与抵抗e次剩余攻击的能力，应尽量平衡，$\xi=2^{-80}$时已比DH协议的PAKE计算时间短。当B缓存公钥时，会更快

**形式化安全性分析**：RSA假设与ROM模型⇒PEKEP与CEKEP在此情景下安全

定义5个混合实验，替换Oracle的响应，将敌手优势降为0（介绍得很详细✓）

$P_0$：真实攻击场景，使用$H_0,H_1,H_2,H_3,H$. $Adv(A)=Adv(A,P_0)$

$P_1$：$H_3$替换为$num\in_R\{0,1\}^k$，与$P_0$的敌手优势很小，归约到RSA问题。

$P_2$：$\Pi_B^j$收到$\Pi_A^i$的send1，接受则$sk\in_R\{0,1\}^k$，与$P_1$差距很小，同样归约到RSA问题

$P_3$：$\Pi_A^i$收到$\Pi_B^j$的send2，同$P_2$优势

$P_4$：$\Pi_A^i$或$\Pi_B^j$收到敌手消息，但敌手猜测仍需解决RSA或穿背随机数，优势仍很小