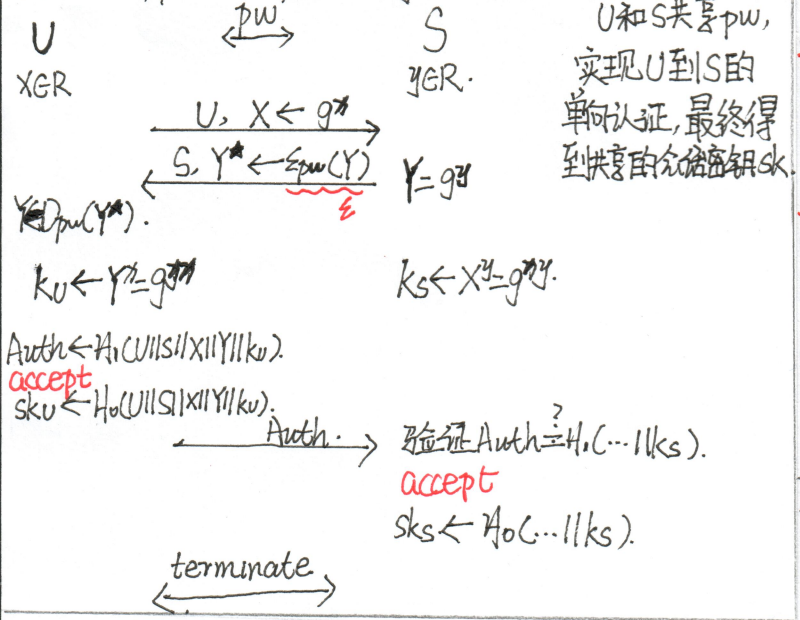
CCS'03 Bresson (OEKE协议(AuthA)+安全性证明).
Security Proofs for an Efficient Password-Based key Exchange

优点：①本文研究了IEEE P1363标准工作组提出的PAKE协议AuthA的安全性分析与证明，基于CDH问题，在random-oracle和ideal-cipher model中证明是安全的，且给出了实现前向安全性的证明；②文章结构、协议图较为清晰，且在结论中提到了本文的不足，为未来工作提供了方向；③提到即使口令不为均匀分布也可证明安全，即将q_p替换为n个最大的概率之和。

问题：①文中协议图Fig1.5，在Client U一侧，均应为accept→true先于sk_U生成，只有实例accept，才会生成sid.pid和sk.
②第1章Introduction的第4段提到无线网络环境中更需要轻量级的认证过程，且未提供密钥交换方法，这一段与上下文没有直接联系，对文章结构无作用。③在语义安全性的证明中，有以下n点可以改进：1.record中多次出现 λ，应给出明确定义。2.在Game G_0中定义事件时应包含后续才定义的$AskH_n$，另外也应给出CDH(X,Y)的式子。

Model（与BPR2000类似）.
1> Query：①Execute(U^i,S^j)：被动窃听。
②Reveal(I)：限I已持有sk且泄露给$\mathcal{A}$才可query
③Send(I,m)：主动攻击(开启会话，拦截重发) q_s次数
2> 安全属性（Freshness，语义安全性，认证），基于CDH完成证明。

One-Encryption key Exchange (OEKE).



U和S共享pw，实现U到S的单向认证，最终得到共享的会话密钥sk.

语义安全性（CDH困难问题下可安全分发sk）.
通过一系列游戏(从真实游戏G_0到G_8)，证明OEKE可抵抗字典攻击，敌手的优势只跟随交互次数的提升而提升.

$$Adv^{ake}_{oeke}(\mathcal{A}) \le 3\times\frac{q_s}{N}+8q_h\times Succ^{cdh}_{\mathcal{G}}(t')+\frac{(2q_e+3q_s+3q_p)^2}{q-1}+\frac{q_h^2+q_{ks}}{2^{\tau_1}}$$

其中$t' \le t+(q_s+q_p+q_e+1)\cdot T_{\mathcal{G}}$

- 在每个Game n中定义事件：
① S_n：当$b=b'$时发生，敌手获得sk.
② Encrypt$_n$：$\mathcal{A}$使用口令加密了数据并进行了提交.
③ Auth$_n$：$\mathcal{A}$生成了Auth，提交并被server接受.
④ AskH：$\mathcal{A}$询问某式子在H_0或H_1下的结果.

G_0：真实攻击游戏(在random-oracle和ideal-cipher model中)
$\mathcal{A}$可使用oracle：H_0.H_1，Σ,$\mathcal{D}$,及所有I，有$Adv^{ake}_{oeke}(\mathcal{A})=2Pr[S_0]-1$
接下来一步步更改oracle的回答方式，游戏终止而$\mathcal{A}$未输出b'，则b'ER或超出了q_s和τ的上界.

G_1：通过一系列Rule仿真H_0.H_1.Σ.$\mathcal{D}$以及所有的I，其中H_0.H_1.Σ.$\mathcal{D}$的记录都存储起来，则除非Σ和$\mathcal{D}$发生碰撞，否则G_0和G_1不可区分. $|Pr[S_1]-Pr[S_0]| \le \frac{q_s^2}{2(q-1)}$.

G_2：更改.S处三里send询问的方式，则敌手加密了数才是，除非该数据之前在Σ询问中获得过，否则G_2和G_1不可区分。$|Pr[S_2]-Pr[S_1]| \le \frac{q_s q_p}{q-1}$，其中$q_s \le q_s+q_p$，即S的实例数.

G_3：通过避免对H_1的询问的碰撞，即与密文的碰撞以及send询问的碰撞，即一旦发生碰撞，游戏终止。除非发生碰撞，否则G_3与G_2不可区分：$|Pr[S_3]-Pr[S_2]| \le \frac{2q_e+q_s}{2(q-1)}+\frac{q_h}{2^{\tau_1+1}}$

G_4：当敌手猜到了pw并用之加密数据给client则中止游戏。通过更改U对该query的响应，若有此记录，则中止，否则正常计算，则，游戏不中止，有G_4和G_3不可区分：$|Pr[S_4]-Pr[S_3]| \le Pr[Encrypt_4]$

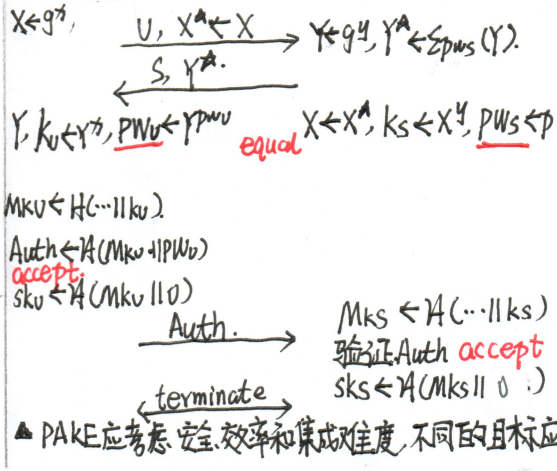
G_5：若敌手未询问H就猜到了Auth则游戏中止，若Auth匹配且有在记录，则游戏中止，否则正常运行。则Auth来自仿真或敌手。除非敌手未询问计算Auth就猜到Auth，否则G_5和G_4不可区分.
$|Pr[S_5]-Pr[S_4]| \le \frac{q_p}{2^{\tau_1}}$

G_6：当敌手猜到口令时终止游戏；若存在$Y^{\mathcal{A}}$的解密记录则中止若$\mathcal{A}$尝试生成Auth，则游戏中止：$Auth_6$发生，否则G_6和G_5不可区分：$|Pr[S_6]-Pr[S_5]| \le Pr[Auth_6]$.

G_7：使用私有的希 H_2和H_3代替H_0和H_1，使Auth和sk与H_0.H_1无关，则只有$\mathcal{A}$询问了H_0.H_1 …||k_U和…||k_S的值(AskH)，否则G_7和G_6不可区分：$|Pr[S_7]-Pr[S_6]| \le Pr[AskH_7]$.
不通过k_U、k_S计算

G_8：通过CDH自归约，通过计算$X=A^x$，$Z=B^y$，若(x,y,X,Y,Z^*)存在于$\Lambda_{\mathcal{G}}$中，则游戏中止，否则记录该值，即等同于已知g^x,g^y直接算出了g^{xy}. 有$Pr[AskH_8] \le q_h Succ^{cdh}_{\mathcal{G}}(t')$.

认证属性的证明类似上述，B附录中有前向安全性的证明.
基于verifier的协议：



▲ PAKE应考虑：安全、效率和集成难度，不同的目标应走门估效分析