TC'16 - Yi Xun - ID2S Password-Authenticated key Exchange Protocols

本文介绍了two-server PAKE协议的原理；给出两个compilers在identity-based cryptography的基石出上，将two-party PAKE转换为two-server PAKE，称为ID2S PAKE协议；在不使用ROM情况下证明安全性；与先前研究相比，性能得到提升。

优点：① 第二章对于协议的定义，描述比较好，可学习论述方式

② 对协议的分析较完整，包括定义，执行流程，安全性分析及性能评估

③ 对PAKE的介绍与分类较好。

问题：① 协议假设口令是均匀随机分布，与实际的分布情况不符。

② 在two-server协议中，存在以下两个问题：1）假设中提到认为两个服务器不会相互勾结，这一点在实际中是否容易保证及实现；2）此类协议，C与两个服务器均建立了会话密钥，最终C与哪个服务器通信未交代清楚，是否可以只有一个服务器通信，另一个负责认证C

③ 协议为客户端带来了较大的开销（相比于前人研究运算时间变长），在实际应用中对客户端的要求较高。

PAKE
- 口令存储在单个服务器上（server compromise有隐患）
  - Password-only PAKE
  - PKI-based PAKE
  - ID-based PAKE
- 口令存储在多个服务器上
  - Threshold PAKE
  - Two-server PAKE

▲ two-server PAKE：客户端将口令分成两个份额（share）分别存储到两个服务器中，两个服务器在未知口令的情况下可以认证客户端，即便攻击者破坏了一个服务器，也无法伪装成客户端通过另一个服务器的认证。

▲ 在identity-based cryptography中，通常使用Private key Generator（PKG）生成私钥，本文方案部署了多个PKG生成私钥并通过安全信道发送给server生成私钥。只要有一个PKG是好的，就可以保证私钥只有服务器可知。（Paterson-ACISP'06）。

▲ 关键建定义（结合Katz'05和Boneh'01的模型定义）。

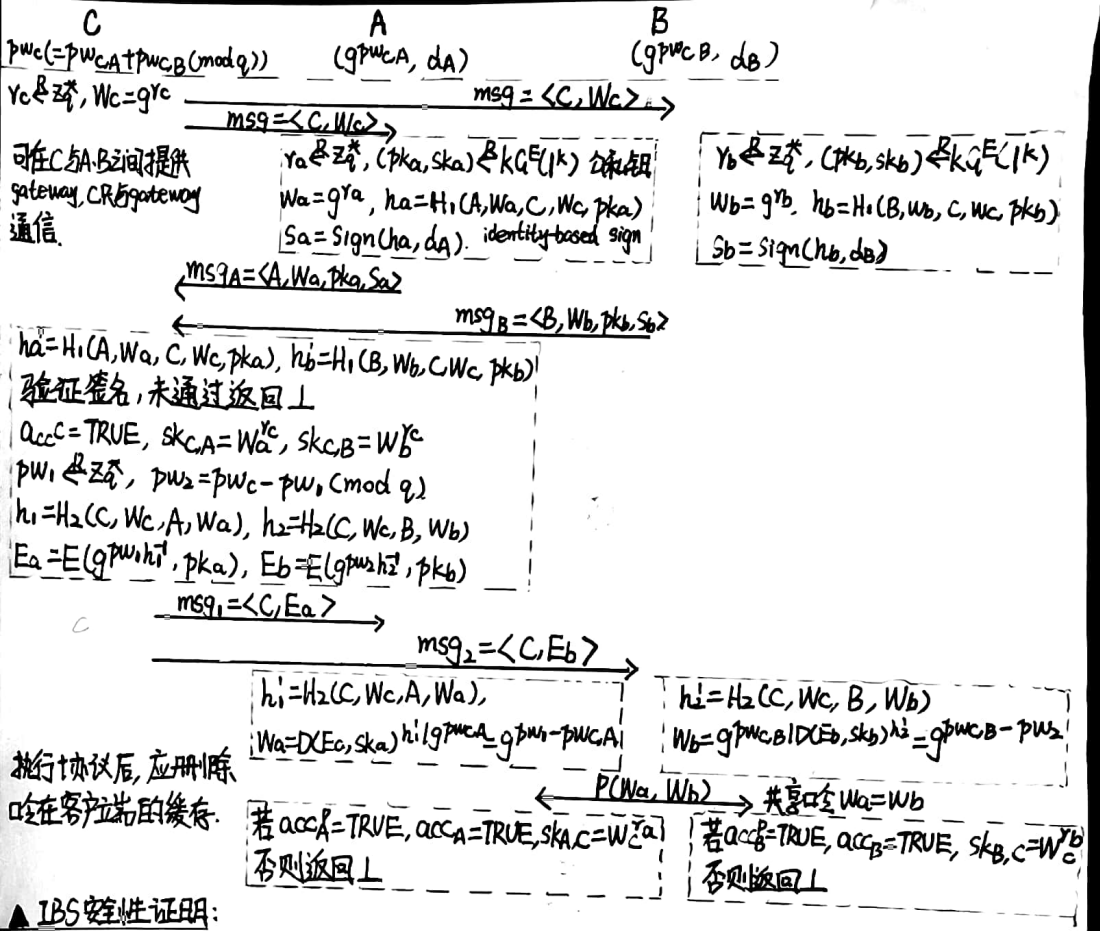
假设：①至少一个PKG正确执行协议 ②两个服务器不会勾结确定口令的值。

ID2S PAKE Protocol（P'，由two-party PAKE协议P转换而来）based on IBS.

Initialization：m个PKG为协议P和IBS生成系统参数和公共参数，确定公钥加密算法E，IBS中有椭圆曲线上的子群，阶为n，E上为循环群。(G, q, g)，$H_1: \{0,1\}^* \to Z_n^*$，$H_2: \{0,1\}^{n+k} \to Z_n^*$；PKG与私密共享$master^{IBS}$，为服务器生成私钥$ds$.

pw_C为客户端口令，存储在服务器上的份额为：$pw_{C,A} + pw_{C,B} = pw_C \pmod q$

口令空间 $N < \min(n, q)$



▲ IBS安全性证明：

基于假设：①对adaptive chosen message攻击者，IBS是不可伪造的 ②E可抵抗选择密文攻击 ③在(G, g, q)上，DDH问题是困难的 ④P是安全的，提供显式认证的PAKE ⑤H_1, H_2抗碰撞

假设攻击者可以corrupt(B)，拿到私钥和口令share.

P_0：协议的真实执行。

P_1：与P_0的不同，当oracle生成的消息重复或H_1, H_2产生的值碰撞时，实验终止，敌手败，$|Adv_A^{P_0}(k) - Adv_A^{P_1}(k)|$ 可忽略 ✓

P_2：与P_1的不同，在Execute$(C, \tau, A, \gamma, B, k)$中，A可能询问corrupt(B)，将$E_A$中的明文$g^{pw_1 h_1}$替换为G中的随机元素，敌手只有打破E的语义安全性才可区别 $|Adv_A^{P_1}(k) - Adv_A^{P_2}(k)|$ 可忽略

P_3：与P_2的不同，将$sk_{C,A}$和$sk_{A,C}$替换为G中相同的随机元素，归约至解DDH问题。

P_4：以上可将Execute的敌手的优势归约为可忽略，P_4中，修改对$Send_1(C, \tau, A, B, msg_A | msg_B)$和$Send(A, \gamma, C, msg_1)$的响应。若$msg_A | msg_B$是敌手生成的，$acc_C = TRUE$，则$msg_A | msg_B$是有效的。若发现$msg_A | msg_B$是敌手生成的且有效，则simulator halt且acc_C赋值为0，和其余情况同P_3。此时认为敌手成功的条件包括acc_C为0的情况，则：$Adv_A^{P_3}(k) \le Adv_A^{P_4}(k)$

P_5：与P_4的不同，在敌手的$Send(A,j,C,msg_1)$中，将E_a中的$g^{pw_1 h^{r'}}$替换为G中的随机值返回，根据P_2易知$|Adv^{P_5}_{\mathcal{A}}(k) - Adv^{P_5}_{\mathcal{A}}(k)|$可忽略

分析P_5：① msg_1是与pw_C独立的，因此无法完成离线字典攻击

② 敌手只能在以下事件发生时才能成功：

a)：敌手query $Send(C,i,A,B,msg_A|msg_B)$，$msg_A|msg_B$是敌手生成的且有效，$acc_C^i = \emptyset, Succ_1$

b)：敌手query $Send(A,j,C,msg_1)$，msg_1是敌手生成的且有效，$acc_A^j = \emptyset$，$Succ_2$.

c) 上述均未发生，敌手通过Test query赢得game.

$Succ_1$：由于msg_A中包含签名S_a，敌手无法找到相同的h_a(抗碰撞)，也无法伪造签名(IBS不可伪造)，故$Pr[Succ_1]$可忽略.

$Succ_2$：假设敌手破坏了B，则有以下3种情况：1) 敌手发现H_2发生碰撞.

2) 敌手更换了E_a中的明文 3) 敌手伪造了msg_1'

1)和2)由假设可忽略，3)中敌手可以猜测正确，服务器收到E_a后生成W_a，在敌手未知W_a的情况下，敌手只能对P做在线猜测.

$Pr[Succ_2] \le \frac{q(k)}{N} + \varepsilon(k)$

故$Pr^{P_5}_{\mathcal{A}}[Succ] \le \frac{q(k)}{N} + \varepsilon(k) + \frac{1}{2}\cdot(1 - q(k)/N - \varepsilon(k))$.

$Adv^{P_5}_{\mathcal{A}}(k) \le Adv^{P_5}_{\mathcal{A}}(k) + \varepsilon(k) \le \frac{q(k)}{N} + \varepsilon(k)$ □.

ID2S PAKE Protocol based on IBE

Initialization：与IBS不同的是，IBE的群G的阶为n，g为生成元.

Password Generation：pw_C仍是均匀随机分布，服务器A,B分别存储$(G^{pw_{C,A}}, g^{pw^*_{C,A}})$和$(G^{pw_{C,B}}, g^{pw^*_{C,B}})$，其中：$pw_{C,A} + pw_{C,B} = pw_C \pmod n$，$pw^*_{C,A} + pw^*_{C,B} = pw_C \pmod q$

安全性证明：

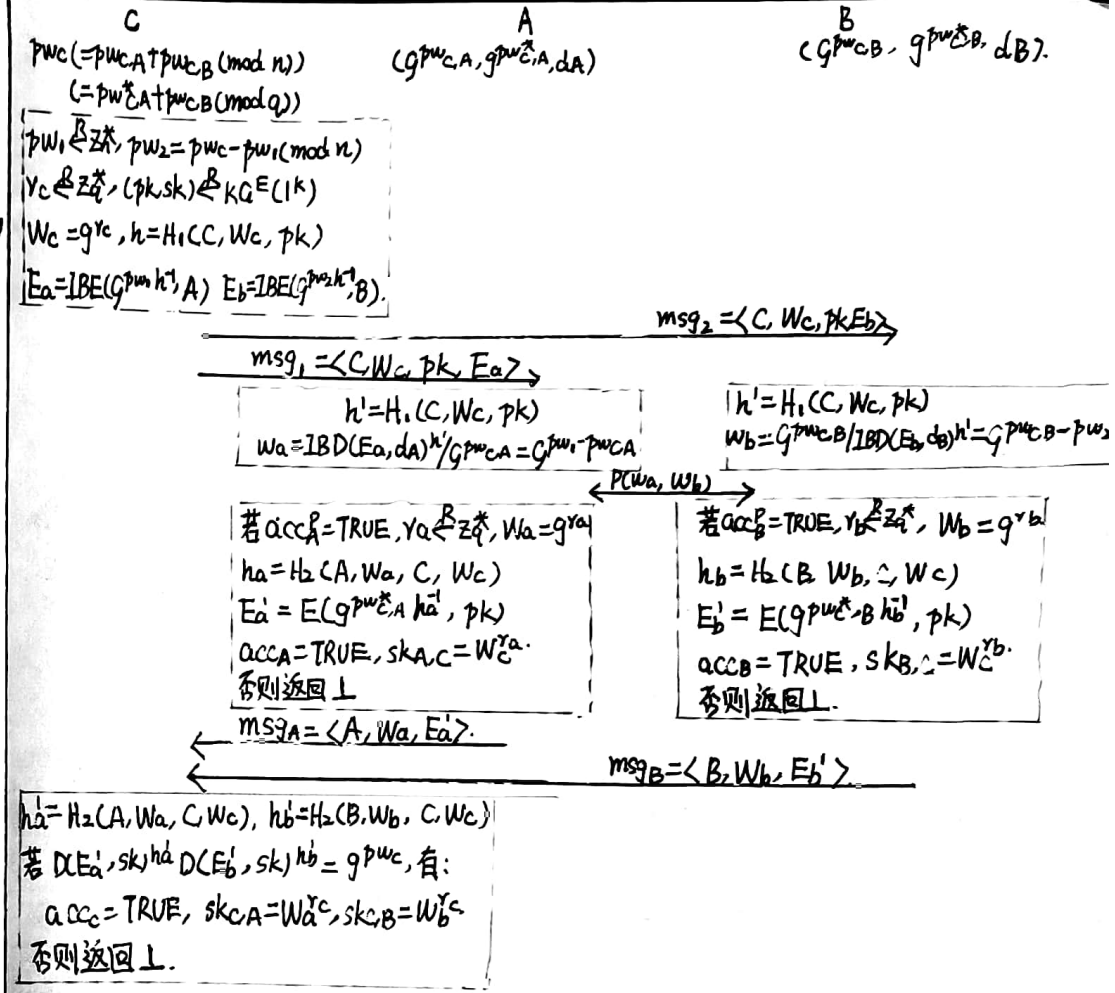
假设①IBE可以抵抗选择密文攻击. ②E也可抵抗选择密文攻击 ③在(G,g,q)上，DDH是困难的 ④P是安全的，提供显式认证的PAKE ⑤H_1, H_2抗碰撞.

P_0：协议的真实执行.

P_1：同IBS的P_1

P_2：更改对$Execute(C,i,A,j,B,k)$的处理，A可能破坏了B，E_a, E_a'中的明文，$sk_{C,A}$和$sk_{A,C}$被替换为G中的随机元素，由于假设①、②，易知$|Adv^{P_2}_{\mathcal{A}}(k) - Adv^{P_1}_{\mathcal{A}}(k)|$可忽略.

P_3：更改对$Send(A,j,C,msg_1)$和$Send(C,i,A,B,msg_A|msg_B)$，同IBS P_4，更改敌手的成功条件，$Adv^{P_3}_{\mathcal{A}}(k)$被$Adv^{P_2}_{\mathcal{A}}(k)$.



P_4：与P_3不同的是，将$Send(A,j,C,msg_1)$和$Send(C,i,A,B,msg_A|msg_B)$的响应更改，用G中随机元素替换$E_a$和$E_a'$中的明文，由假设①、②，$|Adv^{P_4}_{\mathcal{A}}(k) - Adv^{P_3}_{\mathcal{A}}(k)|$可忽略.

对P_4的分析与IBS P_3中的Case 2类似，可得：$Adv^{P_4}_{\mathcal{A}}(k) \le Adv^{P_4}_{\mathcal{A}}(k) + \varepsilon(k) \le q(k)/N + \varepsilon(k)$. □

与Katz方案比较，客户端的性能差，而服务器的计算性能有较大提高.