计算机学报'11 'eCK模型下可证明安全的双方认证密钥协商协议

优点：①提出了新的2AKA协议：SAKA，并在eCK模型下进行了严格的形式化证明 ②协议的描述较为清晰明析。③对协议的安全属性进行详细的分析，并给出密钥确认的解决方案

问题：①2.2节提出eCK模型：CA需验证参与者公钥和身份的绑定情况，而分析3.3.1节的抵抗未知密钥共享攻击却说CA不验证绑定关系，个人分析应是当Sk中不包含身份信息，容易遭受此类攻击，且攻击的描述与图2不一致；②性能分析的描述有些简单，不够有说服力，这点可以改善。③部分描述存在问题：如2.3节的已知密钥安全在后文未出现，对CWPFS的介绍不明确(应从主动和被动攻击角度)，形式化证明的过程可以更详细正式一些。

▲设计可以准确刻画参与者和敌手特征的形式化安全模型，并在该模型下讨论协议的安全性有重要意义。

▲相比于BR模型，Ck模型简化了证明过程，但不能抵抗密钥泄露伪装攻击和双方临时私钥泄露攻击，也不保证wPFS，为弥补上述缺陷，提出了eCK模型。

2AkA的安全目标：1) AKA安全 2) wPFS。

3) 抗密钥泄露伪装攻击

eCK安全模型：

▲参与者：A，B运行的第s次会话为 $\Pi_{A,B}^{s}$

▲ CA：验证参与者长期公钥与身份的绑定情况，通过验证才可参与协议(不验证私钥和公钥的绑定情况)。

▲敌手M，可完全控制通信网络，可做以下预言和查询

1) Send($\Pi_{A,B}^{s}$, m)，M向$\Pi_{A,B}^{s}$发送m，并得到诚实回应，也可要求一方发起对另一方的会话。

2) Long-term-key-Reveal(A)，得到A的长期私钥。

3) Ephemeral-key-Reveal($\Pi_{A,B}^{s}$, A)，得到A在$\Pi_{A,B}^{s}$的临时私钥

4) Session-key-Reveal($\Pi_{A,B}^{s}$)，获取$\Pi_{A,B}^{s}$的会话密钥。

5) Establish-Party(A)，得到A在CA注册的公钥。

6) Test($\Pi_{A,B}^{s}$)，对Fresh的会话做查询，$\Pi_{A,B}^{s}$抛掷硬币b，若b=b，则M得到sk。

▲匹配会话：两个会话的消息互作应答

新鲜性：M未对A，B做1)，3)，且未对$\Pi_{A,B}^{s}$做4)。

协议安全性(语义)：$Adv_{\Pi}^{AKA}(M) = |Pr[b'=b] - \frac{1}{2}|$ 可忽略。

M可对参与双方做长期私钥和临时私钥Reveal，但不可对一个参与者做上述两种Reveal。

SAKA协议：

A私钥a，A为公钥 $A = g^a \bmod p$，IDA为标识。

x为临时私钥，B同A的格式。

A		B
$x, X = H_1(a, x)$		
$k_A = (B)^x \bmod p$		
$s_A = \frac{x}{k_A + a} \bmod q$		
$R_A = g^{k_A} \bmod p$	(R_A, s_A) →	$k_A = (R_A A)^{b s_A} \bmod p = g^{xb} \bmod p$ 验证
		$y, Y = H_1(b, y)$，$k_B = (A)^y \bmod p$
		$s_B = \frac{y}{k_B + b} \bmod q$，$R_B = g^{k_B} \bmod p$
		$k = R_B^{k_A} \bmod p$
$k_B = (R_B B)^{a s_B} \bmod p$	← (R_B, s_B) 验证	$Sk = H(k, s_B, s_A, ID_B, ID_A)$
$k = R_A^{k_B} \bmod p$，Sk		建立Sk

协议满足4个安全属性：

①抵抗未知密钥共享攻击：在Sk中提供身份信息

②抵抗重放攻击：新的Y和y，保证sk的新鲜性

③抵抗冒充攻击：在Sk中包含随机值s_A, s_B(防止敌手生成s并发送)

④弱的完美前向安全性：使用了临时私钥

SAKA-C，使用MAC实现了密钥确认，并提供完美前向安全性。

A → B：(R_A, s_A)

B → A：$(R_B, s_B), MAC_{sk}(e)$，$e = (1, s_A, s_B, ID_A, ID_B)$

A → B：$e' = (0, \cdots)$，$MAC_{sk}(e')$

SAKA的安全性分析：CDH假设，n个参与者，k次会话

若敌手可以$Adv_{\Pi}^{AKA}(M)$优势赢得游戏，则存模拟器S可以在多项式时间以$Adv_{\Pi}^{AKA}(S)$解决CDH，且有

$Adv_{\Pi}^{AKA}(S) \geq \frac{1}{2}\min\{\frac{1}{2^r}Adv_{\Pi}^{AKA}(M), \frac{1}{nk}Adv_{\Pi}^{AKA}(M)\}$。

证：$Sk = H(k, s_A, s_B, ID_A, ID_B)$，M可区分Sk和随机数，只有两种情况

1)密钥复制攻击：M再使参与者加入一个会话，建立相同的Sk，但由于临时私钥不同，且eCk不允许对一个参与者做长期和临时的私钥，故参与者在另一会话产生相同Sk不可能。

2)伪造攻击：M成功算出了k，并通过H得到了Sk。

构造模拟器S，若M可胜利，则S可解决CDH问题，

给S挑战(U, V)，S与M按SAKA协议流程执行，分两种情形

①Test会话有匹配会话(诚实参与者) ②无匹配会话。

①：S随机选A和B参与匹配会话，概率为$\frac{2}{k^2}$

若M可进行该攻击，则可计算k，$k = CDH(U, V)$，

则S可解决CDH问题，则有：$Adv_{\Pi}^{AKA}(S) \geq \frac{2}{k^2}Adv_{\Pi}^{AKA}(M)$

② S随机选B，但未知b，也无法得到长期公钥。

S对B与C(被M控制)的会话：

S为B选临时私钥y，可计算 $k_B = \bar{C}^y \bmod p$，

令 $S_B = h$，为随机值。$U = R_B = g^{k_B} \bmod p$，令SK随机，

M可利用C做运算，验证 k_B'，可知此值不正确，但仍可计算 k_C, S_C, R_C, K。

若M询问 H，则S可将 $S_K = H(K, S_B, S_C, B, C)$ 返回M。

S随后选取会话S，B为应答者，发起者为A。

有 $V = R_A$，则此时M可以成功概率选取S作为Test会话，若M胜利，则一定做了H查询，则S可解。

CDH问题，即有 $Adv_{\Pi}^{AKA}(S) \geq$ 成 $Adv_{\Pi}^{AKA}(M)$

综上有：$Adv_{\Pi}^{AKA}(S) \geq$ 成 $\min\{\frac{1}{K_2} Adv_{\Pi}^{AKA}(M),$ 成 $Adv_{\Pi}^{AKA}(M)\}$