

对 TAKA_{SIP} 协议的分析 and 改进

唐宏斌*, 刘心松

(电子科技大学 计算机科学与工程学院, 成都 610054)

(* 通信作者电子邮箱 tanghongbin@uestc.edu.cn)

摘要: 会话初始化协议(SIP)提供了认证和协商会话密钥,能保证后续会话的安全。2010年,Yoon等(YOON E-J, YOO K-Y. A three-factor authenticated key agreement scheme for SIP on elliptic curves. NSS'10: 4th International Conference on Network and System Security. Piscataway: IEEE, 2010: 334 - 339)提出一种新的三要素 SIP 认证密钥协商协议 TAKA_{SIP}。但 TAKA_{SIP} 协议不能抵抗内部攻击、服务器伪装攻击、离线口令猜测攻击、身份冒充攻击和丢失标记攻击,并且没有提供双向认证。在 TAKA_{SIP} 协议基础上提出一种基于椭圆曲线密码三要素 SIP 认证协议 ETAKA_{SIP} 以解决上述问题。ETAKA_{SIP} 基于椭圆曲线离散对数难题和椭圆曲线密码系统,提供了高安全性。该协议只需 7 次椭圆曲线点乘运算、1 次椭圆曲线加法运算和最高 6 次哈希运算,有较高的运算效率。

关键词: 密码学; 认证协议; 椭圆曲线密码系统; 密钥协商; 会话初始化协议

中图分类号: TN915.04 **文献标志码:** A

Cryptanalysis and improvement of TAKA_{SIP} protocol

TANG Hong-bin*, LIU Xin-song

(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan 610054, China)

Abstract: Session Initiation Protocol (SIP) provides authentication and session key agreement to ensure the security of the successive session. In 2010, Yoon *et al.* (YOON E-J, YOO K-Y. A three-factor authenticated key agreement scheme for SIP on elliptic curves. NSS '10: 4th International Conference on Network and System Security. Piscataway: IEEE, 2010: 334 - 339.) proposed a three-factor authenticated key agreement scheme named TAKA_{SIP} for SIP. However, the scheme is vulnerable to insider attack, server-spoofing attack, offline password attack, and losing token attack. Moreover, it does not provide mutual authentication. To overcome these flaws of TAKA_{SIP}, a new three-factor authentication scheme named ETAKA_{SIP} based on Elliptic Curve Cryptosystem (ECC) was proposed. ETAKA_{SIP}, on the basis of elliptic curve discrete logarithm problem, provides higher security than TAKA_{SIP}. It needs 7 elliptic curve scalar multiplication operations, 1 additional operation and up to 6 Hash operations, and of high efficiency.

Key words: cryptography; authentication protocol; Elliptic Curve Cryptosystem (ECC); key agreement; Session Initiation Protocol (SIP)

0 引言

会话初始协议(Session Initiation Protocol, SIP)是1999年IETF为基于IP的电话协议提出的一种协议^[1],当用户需要使用SIP服务时需要首先向服务器认证,之后才能使用该服务。SIP协议现已广泛应用于超文本传输协议(Hyper Text Transfer Protocol, HTTP)、简单邮件传输协议(Simple Mail Transfer Protocol, SMTP)以及3G移动网络等应用场合中。迄今众学者已提出各种不同的SIP协议^[2-7],但这些协议均存在不同程度的各种攻击或者运行效率问题。2005年,Yang等^[8]指出基于HTTP摘要认证的最初协议存在着离线口令猜测攻击和伪装服务器攻击等,并提出了一种基于离散对数问题和Diffie-Hellman密钥交换算法的方案^[9],但是该方案不适合用于资源有限和低计算能力的场合,而且存在离线口令猜测攻击和Denning-Sacco攻击^[10]。同年,Durlanik等^[11]提出一种基于椭圆曲线密码系统(Elliptic Curve Cryptosystem, ECC)的SIP认证方案,但是该协议仍然存在离线口令猜测攻击和Denning-Sacco攻击。2008年,Tsai等^[12]为了提高协议的执行效率提出基于随机nonce的SIP方案,而2009年Wu

等^[13]也提出一种基于ECC的SIP认证方案,相比之下,Tsai方案比Wu方案和Durlanik方案效率更高,更适合于使用在资源受限的环境。但是Yoon等指出Durlanik协议、Wu协议和Tsai协议中存在着离线口令猜测攻击、Denning-Sacco攻击和被盗验证子攻击(stolen-verifier)。鉴于此,2010年Yoon等^[14]提出了基于椭圆曲线离散对数问题的SIP认证方案TAKA_{SIP},并声称该协议能抵抗各种已知攻击。然而,本文指出TAKA_{SIP}协议仍然存在内部攻击、丢失标记(token)攻击、离线口令猜测攻击和服务器伪装攻击,并提出一种改进的基于椭圆曲线离散对数难题的SIP认证方案ETAKA_{SIP}。椭圆曲线密码系统可以使用更短的系统参数达到传统公钥密码系统的安全性^[15-16],比如系统参数只需要160位即可达到传统的1024位RSA系统安全性,因而ETAKA_{SIP}与TAKA_{SIP}协议相比具有更高的安全性,并保持了TAKA_{SIP}的高效性。

1 TAKA_{SIP} 协议回顾

本章对TAKA_{SIP}协议进行简单介绍并探讨TAKA_{SIP}协议存在的不足。

本文中所使用的符号定义如下:U表示用户;S表示远程

收稿日期:2011-08-15;修回日期:2011-10-03。

作者简介: 唐宏斌(1973-),男,广西河池人,博士研究生,主要研究方向:分布式系统、密码学协议; 刘心松(1940-),男,重庆石柱人,教授,博士,主要研究方向:数字有机体操作系统、数字有机体数据库系统、数字有机体流媒体系统、数字有机体流量调度系统。

服务器; D 表示候选口令字典集; PW 表示口令; B 表示生物特征模板值; k 表示服务器 S 选择的高熵密钥; G_1 表示素数阶 q 的加法交换群; P 表示 G_1 的生成元; Q^* 表示椭圆曲线点 Q 的 x 坐标; xQ 表示椭圆曲线的标量乘法运算即点乘运算; $h(\cdot)$ 表示单向哈希函数; $d(\cdot)$ 表示用于生物特征校验的对称参数函数; τ 表示事先确定的生物特征校验阈值; \parallel 表示字符串连接操作; \oplus 表示异或操作。

1.1 TAKA_{SIP} 协议

TAKA_{SIP} 协议由注册阶段、认证与密钥协商阶段和口令及生物特征修改阶段三阶段组成。

1.1.1 注册

1) $U \rightarrow S: \langle ID, h(ID \parallel PW \parallel B), B \rangle$

用户通过安全信道把 ID , $h(ID \parallel PW \parallel B)$, B 发给服务器 S 。

2) $S \rightarrow U: \langle v, B, h(\cdot), d(\cdot), \tau \rangle$

服务器 S 收到上条消息后计算 $s = h(ID \parallel k)$ 和 $v = s \oplus h(ID \parallel PW \parallel B)$, 并把 $\langle v, B, h(\cdot), d(\cdot), \tau \rangle$ 保存在用户的标记(token)内, 通过安全信道把标记发给用户。

1.1.2 认证和密钥协商阶段

用户希望登录到远程服务器并和服务器协商会话密钥时, 首先输入身份 ID 和口令 PW , 在传感器上输入自己的生物特征值 B^* , 用户的标记首先验证生物特征, 做如下判断: $d(B^*, B) < \tau$, 如果不等式不成立则拒绝登录, 如果成立则继续协议执行。

1) $U \rightarrow S: \text{REQUEST}(ID, A, Mac)$

用户计算 $s = v \oplus h(ID \parallel PW \parallel B)$, 然后选择一个随机数 $a \in \mathbb{Z}_q^*$, 并计算 $A = aP$ 以及 $Mac = h(s \parallel A)$, 然后给服务器发去消息 $\text{REQUEST}(ID, A, Mac)$ 。

2) $S \rightarrow U: \text{CHALLENGE}(nonce, realm, B, AuthS)$

服务器接到 1) 中的消息后, 做如下运算:

① 验证 ID 格式的正确性, 如果格式不正确则服务器停止协议执行, 否则继续执行协议并转下一步;

② 计算 $s' = h(ID \parallel k)$ 并验证 Mac 是否等于 $h(s' \parallel A)$, 如果不相等则服务器停止协议执行, 否则继续;

③ 选择一个随机数 $r \in \mathbb{Z}_q^*$, 并计算 $B = aP, SK_s = bA = abP, AuthS = h(nonce \parallel realm \parallel ID \parallel A^* \parallel B^* \parallel SK_s^*)$;

④ 服务器发送消息 $\text{CHALLENGE}(nonce, realm, B, AuthS)$ 给用户。

3) $U \rightarrow S: \text{RESPONSE}(nonce, realm, AuthU)$

用户接到 2) 中的消息后, 做如下运算:

① 计算 $SK_u = aB = abP$, 并验证 $AuthS$ 是否等于 $h(nonce \parallel realm \parallel ID \parallel A^* \parallel B^* \parallel SK_u^*)$, 如果不相等则停止协议执行, 否则用户认证了服务器的身份并接着往下执行;

② 计算 $AuthU = h(nonce + 1 \parallel realm \parallel ID \parallel A^* \parallel B^* \parallel SK_u^*)$ 并发送消息 $\text{RESPONSE}(nonce, realm, AuthU)$ 给服务器。

4) 服务器接到 3) 中消息后, 验证 $AuthU$ 是否等于 $h(nonce + 1 \parallel realm \parallel ID \parallel A^* \parallel B^* \parallel SK_s^*)$, 如果不相等则停止协议执行, 否则服务器认证了客户的身份并接受用户的认证请求。

协议顺利执行后, 双方协商的一次性会话密钥为 $SK = abP$ 。

1.2 存在的攻击

攻击 1 内部攻击(inside attack)。

当用户在注册阶段给服务器发去 $\langle ID, h(ID \parallel PW \parallel B), B \rangle$ 消息时, 系统管理员可能监听到该消息, 那么管理员可以做如下的离线口令猜测攻击:

1) 从字典集 D 中按顺序选取一候选口令 PW^* ;

2) 计算 $h(ID \parallel PW^* \parallel B)$ 并和 $h(ID \parallel PW \parallel B)$ 值比较, 如果相等则可断定 $PW^* = PW$, 否则转 1) 重新执行。

攻击 2 丢失标记攻击(losing token attack)。

当用户的 token 比如智能卡丢失后, 攻击者可以通过各种攻击获得 token 里面的内容, 包括保存在其中的 v 和 B 值, 如果先前攻击者记录过该用户的通信消息 ID, A, Mac 的内容, 那么攻击者可做如下的离线口令猜测攻击:

1) 从字典集 D 中按顺序选取一候选口令 PW^* ;

2) 计算 $H = h(ID \parallel PW^* \parallel B), s^* = v \oplus H$ 以及 $Mac^* = h(s^* \parallel A)$, 如果 $Mac^* = Mac$ 则可断定 $PW^* = PW$, 否则转 1) 重新执行。

攻击 3 伪装服务器攻击(server spoofing attack)。

TAKA_{SIP} 协议存在着冒充攻击, 具体来说伪装服务器攻击。攻击过程如下:

1) 攻击者 Eve 截获了用户 U 的登录消息 $\text{REQUEST}(ID, A, Mac)$ 。

2) 攻击者 Eve 不作 Mac 验证, 直接选择一个随机数 b , 并计算 $B = bP, SK_s = bA = abP$ 和验证 $AuthS = h(nonce \parallel realm \parallel ID \parallel A^* \parallel B^* \parallel SK_s^*)$, 然后发送消息 $\text{CHALLENGE}(nonce, realm, B, AuthS)$ 给客户。

3) 客户接到该消息后, 计算 $SK_u = abP$ 并验证 $AuthS$ 的正确性。由于计算出的 SK_u 等于 SK_s , 而 $nonce, realm, ID, A, B$ 是双方所共知的, 因此客户对服务器的 $AuthS$ 验证顺利通过, 从而客户“认证”了服务器的身份, 最后客户发送回确认消息给服务器。

从该过程可以看出, 服务器成功地冒充了服务器 S 并和客户协商了随后使用的会话密钥。由此可见, TAKA_{SIP} 协议并未成功地提供双向认证。

2 ETAKA_{SIP} 认证方案

基于椭圆曲线离散对数问题提出新的 ETAKA_{SIP} 认证方案以解决上述不安全的缺陷。协议分为四个阶段: 系统设置阶段、注册阶段、认证和密钥协商阶段以及口令及生物特征改变阶段。

2.1 系统设置阶段

所有用户和服务器协商好如下系统参数: 用户和系统共同选择有限域 $GF(q)$ 上的一条椭圆曲线 $E, E_{a,b}(GF(q))$ 为有限域 $GF(q)$ 上椭圆曲线 E 的一个点加法群, 并设 P 为其生成元, 其阶为 n 。

服务器选择自己的密钥 k , 其对应公钥为 $Q = kP$, 服务器保密 k , 公布其系统参数 q, a, b, n, P, Q 。

2.2 注册阶段

1) $U \rightarrow S: (ID, h(PW \parallel N \parallel B), B)$

用户自由地选择自己的身份 ID 、口令 PW 、新鲜数 N , 然后在传感器上输入自己的生物特征信息 B , 并通过安全信道把 $ID, h(PW \parallel N \parallel B), B$ 发给服务器 S 。

2) $S \rightarrow U: (q, a, b, n, P, Q, v, B, h(\cdot), d(\cdot), \tau)$

服务器 S 收到上条消息后计算 $s = h(ID \parallel k)$ 和 $v = s \oplus h(PW \parallel N \parallel B)$, 并把 $q, a, b, n, P, Q, v, B, h(\cdot), d(\cdot), \tau$ 保存在用户的 token 内, 通过安全信道把 token 发给用户。用户接收到 token 后把 N 输入其内保存。

2.3 认证和密钥协商阶段

当用户希望使用远程服务器上的服务时, 首先要通过普通信道登录服务器并与服务器进行双向认证, 协商随后会话使用的会话密钥。用户首先在自己的 token 上输入 ID, PW 和在传感器上输入生物特征 B^* , 然后进行如下操作:

1) $U \rightarrow S: \text{REQUEST}(ID, R_1, R_2, T_u)$

用户的 token 首先验证 $d(B^*, B) < \tau$ 是否成立, 如不成立则拒绝认证请求; 否则继续计算 $s = v \oplus h(PW \| N \| B)$ 并选择一个随机数 $r_1 \in \mathbb{Z}_q^*$, 计算 $R_1 = (r_1 + T_u \times s)P, R_2 = r_1Q$, 其中 T_u 为 token 当前时钟值。然后 token 给服务器发去消息 $REQUEST(ID, R_1, R_2, T_u)$ 。

2) $S \rightarrow U: RESPONSE(ID, realm, R_3, h_1)$

服务器接到用户发来的 REQUEST 消息后, 首先验证 ID 格式的正确性, 如果格式不正确则停止执行协议; 否则校验 $0 < T_s - T_u < \Delta T$ 是否成立, 其中 T_s 为服务器当前时钟值。如果不等式不成立则服务器停止协议执行, 否则继续往下执行协议。当所有的验证都通过之后, 服务器 S 认证了用户 U 的身份, 因为只有真正的用户 U 才能计算出正确的 R_1, R_2 值, 如果攻击者要冒充用户 U 构造第一条消息, 则将面对椭圆曲线离散对数难题。 S 计算 $R_1' = R_1 - (T_u \times h(ID \| k))P$ 并验证 R_2 是否和 kR_1 相等, 不等则停止执行协议, 否则继续执行协议。 S 随机选择一参数 $r_3 \in \mathbb{Z}_q^*$, 计算出 $R_3 = r_3P, SK_s = r_3R_1' = r_1r_3P, h_1 = h(ID \| S \| R_1 \| R_2 \| R_3 \| SK_s \| h(ID \| k))$ 。最后 S 计算会话密钥 $SK = h(ID \| S \| R_1 \| R_2 \| R_3 \| SK_s)$, 并发送消息 $RESPONSE(ID, realm, R_3, h_1)$ 给用户。

3) 用户接收到 RESPONSE 消息后计算 $SK_u = r_1R_3 = r_1r_3P$, 然后验证 h_1 是否等于 $h(ID \| S \| R_1 \| R_2 \| R_3 \| SK_u \| s)$, 如果不等则用户终止协议执行, 否则用户通过该消息认证了服务器的身份。最后用户 U 计算会话密钥 $SK = h(ID \| S \| R_1 \| R_2 \| R_3 \| SK_u)$ 。

至此, 用户和服务器双方完成了双向认证和密钥协商过程, 最后达成的共同会话密钥为 SK 。在网络状态中等或良好的情况下可以使用如上的认证和密钥协商协议。在网络状态不佳的情况下, 可以修改两消息协议为三消息协议, 去掉时戳因素而加入第三条确认消息, 即设计成标准的 REQUEST、CHALLENGE、RESPONSE 三消息形式协议, 可以去掉全局时钟影响因素。而三消息协议在计算复杂性上仅仅增加了 2 个哈希运算和 1 条通信消息数。

2.4 口令及生物特征修改阶段

当用户由于各种原因要修改口令以及由于生物特征随时间推移而改变时, 用户可以通过本阶段协议修改口令及生物特征值。其修改过程如下:

1) 用户在其 token 上输入身份 ID、口令 PW 以及在传感器上输入自己的生物特征值 B^* 。

2) token 检查 $d(B^*, B) < \tau$ 是否成立, 如果不等式不成立, 则 token 拒绝用户的修改请求; 否则 token 提示用户输入新的口令值。

3) 用户两遍输入口令值 PW^* , 两遍输入是为了保证新口令值的正确性。然后 token 计算 $v^* = v \oplus h(PW \| N \| B) \oplus h(PW^* \| N \| B^*) = (h(ID \| k) \oplus h(PW \| N \| B)) \oplus h(PW \| N \| B) \oplus h(PW^* \| N \| B^*) = h(ID \| k) \oplus h(PW^* \| N \| B^*)$, 同时 token 存储 v^* 值和 B^* 值取代旧的 v 值和 B 值。

3 ETAKA_{SIP} 方案的安全性和性能分析

3.1 ETAKA_{SIP} 安全性分析

定理 1 ETAKA_{SIP} 协议能抵抗重放攻击。

证明 按照 ETAKA_{SIP} 协议的设计思路, 当网络状况良好时不存在时钟窗口问题, 协议只需通过两条消息交互即可完成认证和协商任务。此时因为时戳 T_u 的存在让攻击者无法重放第一条消息, 同时攻击者无法重放第二条消息, 因为该消息含有 R_1 等验证消息在内, 在没有拥有系统密钥 k 或者 $h(ID \| k)$ 的情形下, 攻击者无法正确构造出该消息。

在网络状态不佳的情况下, ETAKA_{SIP} 协议为三消息形式协

议, 此时与两消息协议形式不同的地方是取消了时戳因素而加入第三条确认消息, 服务器可以通过第三条消息确认第一条消息不是重放消息, 而是一个合法用户在实时构造出该消息, 因为只有合法用户才能构造出正确的 RESPONSE 消息。

定理 2 ETAKA_{SIP} 协议能抵抗身份冒充攻击。

证明 攻击者 Eve 无法冒充用户, 因为在不知道 $h(ID \| k)$ 的情况下, Eve 无法正确构造出第一条消息, 因为她要面临 ECDLP 难题; Eve 也无法冒充服务器, 因为在不知道服务器密钥 k 或者 $h(ID \| k)$ 值的情况下, Eve 无法做出正确的回应。

定理 3 ETAKA_{SIP} 协议能抵抗口令猜测攻击。

证明 通过设定一个登录阈值即可遏制在线口令猜测攻击, 因此我们主要考虑离线口令猜测攻击。

情形 1 内部攻击者在监听到 $ID, h(PW \| N \| B)$ 和 B 消息的情形下无法进行口令猜测攻击, 因为哈希值中还包含一个攻击者无法猜测的随机值 N 。

情形 2 从通信中的消息 R_1, R_2, R_3 和 h_1 , 攻击者无法进行离线口令猜测攻击, 因为要从 R_1, R_2 中获得 r_1 和 $h(ID \| k)$ 以及从 R_3 中获得 r_3 值, 则攻击者面临着椭圆曲线离散对数难题; 如果攻击者获得了某个用户的 token 而进行离线口令猜测攻击, 则他只能利用 h_1 进行核对猜测结果, 然而 h_1 中不只含有 $h(ID \| k)$ 值, 而且含有攻击者未知的 SK_u 或者 SK_s 值, 故而攻击者无法用 h_1 进行核对操作, 而要从 R_1, R_2, R_3 求出 SK_u 或者 SK_s 值, 则攻击者将面临椭圆曲线计算 Diffie-Hellman 难题。

情形 3 服务器上并未保存任何关于用户的信息, 故而攻击者无法进行攻破服务器后进行离线口令猜测攻击。

定理 4 ETAKA_{SIP} 协议能抵抗 Denning-Sacco 攻击。

证明 假设攻击者已获得用户某一轮协议执行时的会话密钥 SK , 但是攻击者却因为哈希的单向性而无法推知用户的口令值, 从而 ETAKA_{SIP} 协议能抵抗 Denning-Sacco 攻击。

定理 5 ETAKA_{SIP} 协议能抵抗修改攻击。

证明 因为攻击者无法获得 $h(ID \| k)$, 故而不能正确修改第一条消息。通信中的参数包含在 h_1 中, 同时攻击者也没有系统密钥 k , 故而攻击者也无法修改第二条消息。

定理 6 ETAKA_{SIP} 协议具有完美前向安全性 (Perfect Forward Secrecy, PFS)。

证明 ETAKA_{SIP} 协议使用了 Diffie-Hellman 密钥协商机制, 从而提供了 PFS 特性。

定理 7 ETAKA_{SIP} 协议提供了双向认证性。

证明 从 ETAKA_{SIP} 协议的设计过程可以看出, 协议能提供双向认证性, 第一条信息只有合法的用户才能成功构造出来, 而第二条正确回答的消息除了合法用户外只有服务器才能构造出来, 故而在网络状态良好的情况下通过两条消息提供了双向认证性; 而三消息格式协议在交互最后的确认消息后, 服务器可以确认用户的身份, 因而也提供了双向认证性。

3.2 ETAKA_{SIP} 性能分析

性能分析主要考虑认证和密钥协商阶段的计算代价, 而其中计算代价最大的是椭圆曲线上的点乘运算, 异或运算所需时间可以忽略。TAKA_{SIP} 和 ETAKA_{SIP} 协议的计算代价和通信代价比较如表 1 所示。

表 1 TAKA_{SIP} 和 ETAKA_{SIP} 协议的计算代价和通信代价比较

协议	计算代价	通信代价 (消息数)
TAKA _{SIP}	4PM + 8H	3
ETAKA _{SIP}	7PM + 1PA + 4H	2
	7PM + 1PA + 6H*	3*

表 1 中 M 代表椭圆曲线上标量乘法即点乘运算, PA 代

表点加运算, H 代表哈希运算; * 表示该代价为三消息格式协议所需代价。

表2 TAKA_{SIP}和 ETAKA_{SIP}的安全性能比较

攻击类型及安全属性	TAKA _{SIP}	ETAKA _{SIP}
抵抗内部攻击	否	是
抵抗 Stolen-verifier 攻击	是	是
抵抗重放攻击	是	是
抵抗身份冒充攻击	否	是
抵抗离线口令猜测攻击	否	是
抵抗 Denning-Sacco 攻击	是	是
提供会话密钥协商	是	是
提供完美前向安全	是	是
提供双向认证	否	是

4 结语

Yoon 等提出的 TAKA_{SIP} 协议结合了口令、token 和生物特征三者以提供基于三要素的认证安全性,该方法和传统基于口令的认证方案比较提供了高安全性和高运算效率。然而 TAKA_{SIP} 协议仍不能抵抗内部攻击、服务器伪装攻击、离线口令猜测攻击、身份冒充攻击和丢失 token 攻击,而且没有提供双向认证。本文提出一种基于椭圆曲线密码三要素 SIP 认证协议 ETAKA_{SIP},该协议基于椭圆曲线运算,通过椭圆曲线离散对数难题和时戳因素使非法用户无法正确构造出或重放登录消息,而服务器在回复消息中必须嵌入所拥有的私密信息,并通过 Diffie-Hellman 密钥交换机制协商会话密钥,因此该协议能抵抗 TAKA_{SIP} 协议所遭受的各种攻击,从而更加安全。TAKA_{SIP} 协议的认证及密钥协商协议部分在运行过程中需要 8 次哈希运算和 4 次椭圆曲线点乘运算,本协议的认证及密钥协商协议部分需 7 次椭圆曲线点乘运算、1 次椭圆曲线加法运算和 6 次哈希运算,本协议保持了 TAKA_{SIP} 协议的高效性。

参考文献:

- [1] ROSENBERG J, SCHULZKRINNE H, CAMARILLO G, *et al.* IETF RFC3261, SIP: session initiation protocol [S]. IETF, 2002.
- [2] THOMAS M. IETF Internet Draft, draftthomas-sip-sec-reg-00.txt, SIP security requirements [S]. IETF, 2001.
- [3] SALSANO S, VELTRI L, PAPALILLO D. SIP security issues: the

SIP authentication procedure and its processing load [J]. IEEE Network, 2002, 16(6): 38-44.

- [4] GENEIATAKIS D, DAGIUKLAS T, KAMBOURAKIS G, *et al.* Survey of security vulnerabilities in session initiation protocol [J]. IEEE Communication Surveys and Tutorials, 2006, 8(3): 68-81.
- [5] YOON E-J, YOO K-Y. Cryptanalysis of DS-SIP authentication scheme using ECDH [C]// NISS'09: International Conference on New Trends in Information and Service Science. Piscataway: IEEE, 2009: 642-647.
- [6] YOON E-J, YOO K-Y. A new authentication scheme for session initiation protocol [C]// CISIS'09: International Conference on Complex, Intelligent and Software Intensive Systems. Piscataway: IEEE, 2009: 549-554.
- [7] ARSHAD R, IKRAM N. Elliptic curve cryptography based mutual authentication scheme for session initiation protocol [C]// Multimedia Tools and Applications. Berlin: Springer-Verlag, 2011: 1-14.
- [8] YANG C C, WANG R C, LIU W T. Secure authentication scheme for session initiation protocol [J]. Computers and Security, 2005, 24(5): 381-386.
- [9] DIFFIE W, HELLMAN M E. New directions in cryptography [J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.
- [10] DENNING D, SACCO G. Timestamps in key distribution systems [J]. Communications of the ACM, 1981, 24(8): 533-535.
- [11] DURLANIK A, SOGUKPINAR I. SIP authentication scheme using ECDH [J]. World Enformatika Society Transaction on Engineering Computing and Technology, 2005, 8: 350-353.
- [12] TSAN L. Efficient nonce-based authentication scheme for session initiation protocol [J]. International Journal of Network Security, 2009, 9(1): 12-16.
- [13] WU LUFU, ZHANG YUQING, WANG FENGJIAO. A new provably secure authentication and key agreement protocol for SIP using ECC [J]. Computer Standard & Interfaces, 2009, 31(2): 286-291.
- [14] YOON E-J, YOO K-Y. A three-factor authenticated key agreement scheme for SIP on elliptic curves [C]// NSS '10: 4th International Conference on Network and System Security. Piscataway: IEEE, 2010: 334-339.
- [15] KOBLITZ N. Elliptic curve cryptosystems [J]. Mathematics of Computation, 1987, 48(177): 203-209.
- [16] MENEZES A J, van OORSCHOT P C, VANSTONE S A. Handbook of applied cryptography [M]. New York: CRC Press, 1997.

(上接第 467 页)

式可否认源认证方案。分析表明,该协议不仅满足可否认源认证协议的基本要求,接收方可以认证数据源,但不能向第三方证实发送方的真实身份;而且能够保证明文的神秘性。利用随机预言模型,在基于 CDH 问题是难解的假设下,本文证明了方案的安全性。方案基于身份设计,使用双线性对函数,故可以使用短密钥,设计简单,可使用在计算能力、存储空间受限的设备上。事实上,如何利用 CDH 问题以及 BDH(判定 Diffie-Hellman)问题(包括它们的变形)的难解性,来设计更多可证安全、有效的基于身份的认证方案是一个非常意义的课题,也是作者下一步要进行的工作。

参考文献:

- [1] CANETTI R, DWORK C, NAOR M, *et al.* Deniable encryption [C]// Advances in Cryptology—CRYPTO '97, LNCS 1294. Berlin: Springer-Verlag, 1997: 165-179.
- [2] DWORK C, NAOR M, SAHAI A. Concurrent zero-knowledge [C]// STOC '98: Proceedings of the 30th Annual ACM Symposium on Theory of Computing. New York: ACM, 1998: 409-418.
- [3] AUMANN Y, RABIN M. Efficient deniable authentication of long messages [EB/OL]. [2011-04-05]. <http://www.cs.cityu.edu>.

hk/dept/video.html.

- [4] DENG X, LEE C H, ZHU H. Deniable authentication protocols [J]. IEE Proceedings: Part E: Computers and Digital Techniques, 2001, 148(2): 101-104.
- [5] FAN LEI, XU CHANGXIANG, LI JIANHUA. Deniable authentication protocol based on Diffie-Hellman algorithm [J]. IEE Electronics Letters, 2002, 38(4): 705-706.
- [6] SHAO ZUHUA. Efficient deniable authentication protocol based on generalized ElGamal signature scheme [J]. Computer Standards and Interfaces, 2004, 26(1): 449-454.
- [7] LU RONGXING, CAO ZHENFU. A new deniable authentication protocol from bilinear pairings [J]. Applied Mathematics and Computation, 2005, 168(2): 954-961.
- [8] LU RONGXING, CAO ZHENFU. Non-interactive deniable authentication protocol based on factoring [J]. Computer Standards & Interfaces, 2005, 27(4): 401-405.
- [9] LEE W-B, WU C-C, WOEI J-T. A novel deniable authentication protocol using generalized ElGamal signature scheme [J]. Information Sciences, 2007, 177(1): 1376-1381.
- [10] 武涛,郑雪峰,姚宣霞,等.一种新的高效的可否认源认证协议 [J]. 小型微型计算机系统, 2008, 29(10): 1786-1788.