

一种新的三方认证密钥协商协议

潘操, 丁辉, 王洪元

(常州大学 信息科学与工程学院, 江苏 常州 213164)

摘要: 目前大部分基于身份的三方认证密钥协商协议都存在安全缺陷, 文中在 Xu 等人提出的加密方案的基础上, 设计了一种基于身份的三方认证密钥协商协议. 该协议的安全性建立在 BDDH 假设基础上, 经安全性分析, 协议具有已知密钥安全, PKG 前向安全, 并能抵抗未知密钥共享攻击和密钥泄露伪装攻击, 因此该协议是一个安全的三方密钥协商协议.

关键词: 基于身份的; 双线性对; 三方认证密钥协商协议

中图分类号: TP39

文献标识码: A

文章编号: 1000-7180(2011)07-0143-03

A New Identity-Based Tripartite Authenticated Key Agreement Protocol

PAN Cao, DING Hui, WANG Hong-yuan

(School of Information, Changzhou University, Changzhou 213164, China)

Abstract: Now, most of the tripartite authenticated key agreement protocols have been proven to be insecure. We design the new identity-based tripartite authenticated key agreement protocol, it is based on the secure IBE scheme by Peng. This protocol's security based on bilinear decisional Diffie-Hellman assumption. This protocol could provide known key security, PKG forward secrecy, key-compromise impersonation resilience and unknown key-share resilience, so it's a secure tripartite authenticated key agreement protocol.

Key words: identity-based; bilinear pairings; tripartite authenticated key agreement protocol

1 引言

随着无线网络的普及, 需要通过无线网络传递的信息量迅速增加, 传递过程中信息的安全性尤为重要. 密钥协商协议是一种保护信息安全的重要网络安全协议. 通过该协议通信中的双方或多方能共同协商出一个共享的会话密钥. 在协商的过程中, 每一方都对会话密钥有所贡献, 但是任何一方也不能控制密钥成为一个特定的值.

文献[1]提出了公钥密码学的概念和第一个密钥协商协议——Diffie-Hellman 协议. 文献[2]利用椭圆曲线上双线性提出了第一个三方密钥协商协议, 但是 Shim^[3]指出 Joux 协议是不可认证的, 容

易受到中间人攻击(man-in-the-middle attack). 随后, 许多学者对三方密钥协商协议展开研究. 但是目前大部分三方密钥认证协议^[4,5]都是不安全的. 文中在文献[6]基础上提出了一种新的基于身份的加密方案, 设计了一种新的基于身份认证密钥协商协议, 该协议的安全性是建立在 BDDH(Bilinear Decisional Diffie-Hellman)假设基础上.

2 背景知识

2.1 安全 AK 协议

一个安全的密钥协商协议要能够抵御主动攻击(攻击者通过拦截、删除、消息重放等手段破坏通信)和被动攻击(攻击者仅通过观察诚实主体的行为试

收稿日期: 2010-11-23; 修回日期: 2010-12-20

基金项目: 国家自然科学基金项目(61070121, 60973094, 60973094); 江苏省产学研前瞻性联合研究项目(BY2009117); 江苏省常州市过程感知与互联技术重点实验室项目

图阻止协议的执行). 除此之外, 一个理想的 AKC 协议还要具备各种安全特性^[7].

2.2 双线性对

设 G_1, G_2 分别是阶为素数 p 的加法群和乘法群, p 为 G_1 的一个生成元. 双线性对 $\hat{e}: G_1 \times G_2 \rightarrow G_2$ 为具有如下性质的映射:

(1) 双线性:

$$\hat{e}(P+Q, R) = \hat{e}(P, R)\hat{e}(Q, R), \hat{e}(P, Q+R) = \hat{e}(P, Q)\hat{e}(P, R), \hat{e}(aP, bR) = \hat{e}(P, Q)^{ab}, \text{ 对所有的 } P, Q, R \in G_1, ab \in Z_q^*.$$

(2) 非退化性: $\hat{e}(P, Q) \neq 1, 1$ 是 G_2 的单位元;

(3) 可计算性: 存在有效算法可以计算 $\hat{e}(P, Q)$, 对所有的 $P, Q \in G_1$.

3 Xu 等的加密方案

Xu 等^[6] 在 2008 年提出了基于身份的加密方案, 该方案的加密过程如下:

(1) 建立阶段

给定一个安全参数 k , 产生一个素数 $q, q = 2q' + 1$, 其中 q' 是一个足够大的素数. G_1, G_2 是以 q 为阶的群, $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 是一个双线性对. P 是 G_1 的生成元.

随机选择 $a \in Z_q^*$, 计算 $P_{Enc} = a \cdot P \in G_1^*$; 随机选择一个主私钥 $s \in Z_q^*$, 计算 $s \cdot P_{Enc}$.

选择三个安全的 hash 函数: $H_1: G_2 \rightarrow \{0, 1\}$, $H_2: \{0, 1\}^{2 \times |q|} \rightarrow Z_q^*$, $H_3: \{0, 1\}^* \rightarrow G_1^*$.

系统参数为 $q, G_1, G_2, \hat{e}, P, P_{Enc}, s \cdot P_{Enc}, H_1, H_2, H_3$.

(2) 私钥生成阶段

对于一个身份为 ID 的用户, 令 PK_{ID}, SK_{ID} 为他的公私钥对. 其中 $PK_{ID} = H_3(ID) \in G_1^*, SK_{ID} = s \cdot PK_{ID} \in G_1^*$.

(3) 加密阶段

随机选择 $\sigma \in Z_q^*$, 使用接收者的公钥 PK_{ID} 将密文设置成:

$$c = \langle \hat{e}(P, P)^{H_2(\sigma, m)}, H_2(\sigma, m)P_{Enc}, H_1(\hat{e}(P, P)^{H_2(\sigma, m)} \cdot \hat{e}(H_2(\sigma, m)PK_{ID}, s \cdot P_{Enc})) \oplus \sigma, H_1(\hat{e}(H_2(\sigma, m)PK_{ID}, s \cdot \sigma \cdot P_{Enc})) \oplus m \rangle$$

(4) 解密阶段

将密文 c 分解成 c_1, c_2, c_3, c_4 . 解密过程如下:

计算 $\sigma' = H_1(c_1 \cdot \hat{e}(SK_{ID}, c_2)) \oplus c_3, m' = H_1(\hat{e}(SK_{ID}, \sigma \cdot c_2)) \oplus c_4$; 如果

$c_1 = \hat{e}(P, P)^{H_2(\sigma', m')}, c_2 = H_2(\sigma', m')P_{Enc}$ 不成立, 则输出 $\perp$. 显然, 如果密文 c 有效, 则 $m = m'$.

4 新的三方密钥协商协议

本协议仍然是由系统建立阶段, 私钥生成阶段和密钥协商阶段这三个阶段组成, 符号的使用与双方密钥协商协议一致. 假设三个用户 A、B、C 希望通过本协议协商达成一个会话密钥. 在系统建立阶段发布系统参数: $\{q, G_1, G_2, \hat{e}, P, P_{Enc}, s \cdot P_{Enc}, H_1, H_2, H_3\}$; 在私钥生成阶段由私钥生成中心 PKG 为用户 A、B、C 分别颁发公私钥对 $(PK_A, SK_A), (PK_B, SK_B), (PK_C, SK_C)$, 其中 $PK_A = H_3(ID_A), SK_A = s \cdot PK_A, PK_B = H_3(ID_B), SK_B = s \cdot PK_B, PK_C = H_3(ID_C), SK_C = s \cdot PK_C$. 协议执行过程如图 1 所示.

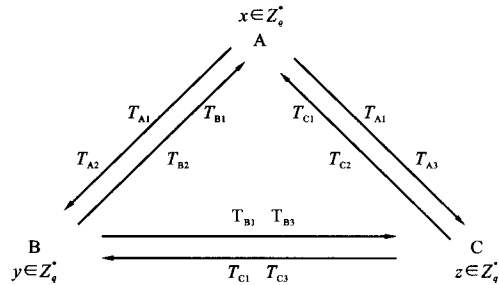


图 1 新的基于身份的三方协议

(1) 用户 A 随机选择一个数 x 作为他的临时私钥, 并计算:

$$T_{A1} = x \cdot H_2(x, xP_{Enc})P_{Enc}, T_{A2} = H_1(\hat{e}(H_2(x, xP_{Enc})PK_B, sxP_{Enc})) \oplus P_{Enc}, T_{A3} = H_1(\hat{e}(H_2(x, xP_{Enc})PK_C, sxP_{Enc})) \oplus P_{Enc}, \text{ 将 } T_{A1}, T_{A2} \text{ 发送给用户 B, 将 } T_{A1}, T_{A3} \text{ 发送给用户 C;}$$

(2) 用户 B 随机选择一个数 y 作为他的临时私钥, 并计算:

$$T_{B1} = y \cdot H_2(y, yP_{Enc})P_{Enc}, T_{B2} = H_1(\hat{e}(H_2(y, yP_{Enc})PK_A, syP_{Enc})) \oplus P_{Enc}, T_{B3} = H_1(\hat{e}(H_2(y, yP_{Enc})PK_C, syP_{Enc})) \oplus P_{Enc}, \text{ 将 } T_{B1}, T_{B2} \text{ 发送给用户 A, 将 } T_{B1}, T_{B3} \text{ 发送给用户 C;}$$

(3) 用户 C 随机选择一个数 z 作为他的临时私钥, 并计算:

$$T_{C1} = z \cdot H_2(z, zP_{Enc})P_{Enc}, T_{C2} = H_1(\hat{e}(H_2(z, zP_{Enc})PK_A, szP_{Enc})) \oplus P_{Enc}, T_{C3} = H_1(\hat{e}(H_2(z, zP_{Enc})PK_B, szP_{Enc})) \oplus P_{Enc}, \text{ 将 } T_{C1}, T_{C2} \text{ 发送给用户 A, 将 } T_{C1}, T_{C3} \text{ 发送给用户 B;}$$

(4) 用户 A 计算: $K_{ABC} = \hat{e}((H_1(\hat{e}(SK_A, T_{B1})) \oplus T_{B2}, H_1(\hat{e}(SK_A, T_{C1})) \oplus T_{C2}))^x$; 用户 B 计算: $K_{BAC} = \hat{e}((H_1(\hat{e}(SK_B, T_{A1})) \oplus T_{A2}, H_1(\hat{e}(SK_B, T_{C1})) \oplus T_{C3}))^y$; 用户 C 计算: $K_{CAB} = \hat{e}((H_1(\hat{e}(SK_C, T_{A1})) \oplus T_{A2}, H_1(\hat{e}(SK_C, T_{B1})) \oplus T_{B3}))^z$.

$$T_{A1})) \oplus T_{A3}, H_1(\hat{e}(SK_C, T_{B1})) \oplus T_{B3})^z.$$

显然, $K_{ABC} = K_{BAC} = K_{CAB} = \hat{e}(P, P)^{a^2xyz}$;

(5) 最终的会话密钥:

$$sk = PK_A \parallel PK_B \parallel PK_C \parallel K_{ABC}$$

5 新协议的安全性分析

(1) 已知密钥安全(know-key security): 协议的每一轮所产生的会话密钥都不相同. 每执行一次新密钥协商协议, 参与的三方都会随机选择一个临时私钥, 利用该临时私钥计算会话密钥. 因此, 即使攻击者获得了其它几次会话密钥, 也不会威胁到本次协议执行所产生的会话密钥的安全性.

(2) 完美前向安全(forward secrecy): 在协议的执行过程中, 如果参与的三方中有一方或有几方的长期私钥丢失, 并不影响他们先前所达成的会话密钥的安全. 因为攻击者即使获得了参与者的长期私钥, 由于他无法获知先前协议执行过程中, 参与者所使用的临时私钥, 所以他也无法恢复参与者先前所达成的会话密钥.

(3) PKG 前向安全 (PKG Forward Secrecy, PKG-FS): 对于本协议, 若在某一时刻, PKG 的主私钥(master key)泄露, 获得该主私钥的攻击者仍然不能够求出该 PKG 的用户之前协商获得的会话密钥. 因为攻击者要求出该 PKG 用户先前协商所达成的会话密钥, 必须要知道先前协议执行时, 参与者所使用的临时私钥. 同时即使获得主私钥的攻击者通过不安全信道截获参与者发送的信息, 但是它无法计算出参与者所使用的临时私钥, 因此也无法计算出会话密钥.

(4) 抗密钥泄露伪装攻击(key-compromise impersonation): 如果参与者 A 的长期密钥泄露, 获得这个密钥的攻击者 E 想对 A 冒充其它诚实实体, 如参与者 B. 由于攻击者 E 只知道 A 的长期私钥, 并不知道其他参与实体的长期私钥, 所以他无法在 A 面前伪装成其它诚实实体.

(5) 抗未知密钥共享攻击(unknown key-share): 如果攻击者 E 想在诚实的参与者 A 面前扮演诚实的参与者 E, 而在诚实的参与者 B 面前扮演诚实的参与者 A, 这是不可能达成的. 因为, 在协议的执行过程隐含了身份的认证, 并且在最后达成的会话密钥中包含了身份的认证. 同时, 用户公钥的产生使用了 hash 函数, 攻击者很难伪造.

(6) 密钥控制(key control): 由于最后的会话密钥是由参与三方共同协商的, 包括所有参与者的临时私钥, 因此任何一方都不能单独决定会话密钥.

6 结束语

文中利用 Xu 的加密方案提出了一种新的基于身份的三方密钥协商协议. 经过安全性能分析, 该协议具有已知密钥安全、完美前向安全、PKG 前向安全、抗密钥泄露伪装攻击、抗未知密钥共享攻击、密钥控制安全, 是一个安全的三方认证密钥协商协议.

参考文献:

- [1] Diffie W, Hellman M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.
- [2] Joux A. A one-round protocol for tripartite diffie-hellman [C]// Proceedings of the 4th International Algorithmic Number Theory Symposium (ANTS-IV), London, UK: Springer-Verlag, 2000: 385-394.
- [3] Shim K. Efficient one-round tripartite authenticated key agreement protocol from weil pairing [J]. Electronics Letters, 2003, 39(2): 208-209.
- [4] Chen Z. Security analysis of Nalla-Reddy's ID-based tripartite authenticated key agreement protocols [EB/OL] [2010-03-13]. <http://eprint.iacr.org/>, #2003/103, 2003.
- [5] Nalla D, Reddy K C. ID-based tripartite Authenticated Key Agreement Protocols from pairings, Cryptology ePrint Archive: Report, (004)(2003). [D] India: University of Hyderabad, 2003.
- [6] Peng Xu, Guo-Hua Cui. An efficient and provably secure IBE scheme with short system parameters. wireless communications [C]// proceedings of the 4th International Conference on wireless Communications, Networking and Mobile Computing. Dalian China: [s.n], 2008.
- [7] Wilson B, Johnson D, Menezes A. Key agreement protocols and their security analysis [C]// Proceedings of the 6th IMA International Conference on Cryptography and Coding. Heideelberg: Springer-Nerlag, 1997: 30-45.

作者简介:

潘操 男, (1977-), 讲师. 研究方向为计算机网络安全及应用.

王洪元 男, (1960-), 博士, 教授, 硕士生导师. 研究方向为智能系统与物联网技术应用.