新的可证明安全的快速认证协议

朱 辉，李 晖，庞辽军，王育民

(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

【摘要】利用Canetti-Krawczyk模型构造了一个快速认证协议，并对该协议的安全性进行了详细的分析和证明。分析表明，该协议实现了Canetti-Krawczyk模型下可证明安全的快速身份认证、密钥协商和密钥更新，且具有双向实体认证、完美的向前保密性等安全属性，满足了认证的安全需求。该认证协议仅需进行2轮交互即可完成，通信开销小，计算量较低，为用户间的相互认证提供了一种高效的解决方案。

关 键 词 认证协议； Canetti-Krawczyk模型； 可证明安全； 安全分析.
中图分类号 TP309 **文献标识码** A

New Provable Security Fast Authentication Protocol

ZHU Hui, LI Hui, PANG Liao-Jun, and WANG Yu-Min

(Ministry of Education Key Laboratory of Computer Network and Information Security, Xidian University Xi'an 710071)

Abstract With Canetti-Krawczyk model, a fast authentication protocol of exchanging multiple session keys between two participants is proposed. The security analysis and formal proof show that the proposed protocol is session-key secure with perfect forward secrecy (PFS). Moreover, the implementation of the protocol just need twice communications and a little computation. The results show the efficiency of the protocol in wireless network.

Key words authentication protocol; Canetti-Krawczyk model; provable security; security analysis

随着无线网络的快速发展，快速认证协议已经成为近年来密码学研究的热点之一。由于无线网络的特殊性，要求认证协议在保证安全性的前提下，通信交互和计算量要尽可能地少。文献[1-7]分别通过不同方法来实现安全的认证协议，但是在通信和计算上的开销都比较大。

本文在分析当前研究结果的基础上，提出一种快速认证协议，该协议采用模块化的设计方式，在Canetti-Krawczyk(简称CK)模型[8]下可证明安全，具有所需的安全性质。

1 Canetti-Krawczyk模型简介

Canetti-Krawczyk模型是一种用于形式化分析密钥交换协议的工具，该模型采用模块化[9]的方法设计和分析密钥交换协议，利用计算不可区分性[10]的概念定义安全性。

1.1 非认证链路攻击模型(UM)

UM中的攻击者Adv除能够控制通信链路和协议事件的调度外，还能通过明确的攻击手段来得到协议参与者存储器中的秘密信息。CK模型将攻击分为攻陷参与者、会话密钥查询、会话状态暴露3类。

1.2 认证链路模型(AM)

AM的定义方式与UM完全一样，但AM中的攻击者只能传递由参与者产生的真实消息，不能改变或增添消息的内容。

1.3 认证器(authenticator)

认证器是一种特殊的算法，它能将AM中的协议转化为UM中等价(安全性相同)的协议。

若编译器C对任何AM中的协议π、协议$C(\pi)$都可以在UM中模仿π，则称该编译器为认证器。

消息传输认证器(message transfer authenticator)，实现认证用户间简单的消息交换。

定理 1[2] 假设λ是一个消息传输认证器，C^{λ}是基于λ的编译器，则C^{λ}是一个认证器。

1.4 测试会话查询和密钥交换协议对手

测试会话查询[11]即Adv可以在它运行的任何时刻，从已完成的、没过期的、未暴露的会话中选择一个作为测试会话。设k是该会话的会话密钥，当Adv

收稿日期：2007 – 09 –24；修回日期：2008 – 05 – 28
基金项目：国家自然科学基金(60772136, 60803151)；国家863计划(2007AA01Z435)；高等学校学科创新引智计划(B08038).
作者简介：朱 辉(1981 –)，男，讲师，博士生，主要从事无线网络安全和可证明安全方面的研究.

测试会话查询时，掷币b，$b \xleftarrow{R} \{0,1\}$，若$b=0$，把k给Adv；否则，从协议产生密钥的概率分布空间随机选择一个值给Adv，Adv不允许对该会话和与其匹配的会话发动会话状态暴露、会话密钥查询或者是攻陷参与者攻击。最后，Adv输出一个比特b'，作为对b的猜测。

对于允许测试会话查询的攻击者，CK模型将其称之为密钥交换协议对手。

1.5 会话密钥安全性定义

定义 1[2] 如果对于UM(AM)中的任何密钥交换协议对手Adv，协议能够满足下列两条性质，称该协议在UM(AM)中是会话密钥安全的。

(1) 如果两个未被攻陷的参与者完成了匹配的会话，它们将输出相同的会话密钥；

(2) Adv进行测试会话查询，猜中b的概率不超过$0.5+\varepsilon$，其中ε为安全参数下可忽略的概率。

定理 2[2] 设π在AM中是会话密钥安全的密钥交换协议，λ是消息传输认证器，则$\pi' = C^{\lambda}(\pi)$在UM中是会话密钥安全的密钥交换协议。

2 构造CK模型下安全的认证协议

2.1 构造AM下会话密钥安全的认证协议$\mathbf{SKP_{AM}}$

参数设置：设p、q为素数，$q|p-1$，g是群Z_p^*中阶为q的元素；发起方为A，响应方为B；$H:\{0,1\}^{\infty} \to \{0,1\}^n$为安全Hash函数。

(1) A随机选$x \in Z_p^*$，发送消息$(A,B,s,a=g^x)$给B；

(2) B收到消息后，随机选择$y \in Z_p^*$，发送消息$(A,B,s,b=g^y)$给A，$r=a^y=g^{xy}$，删除y，并输出会话密钥$K=H(g^{xy}\|A\|B)$，会话标示为s；

(3) A收到消息后，计算$r'=b^x=g^{xy}$，删除x，输出会话密钥$K=H(g^{xy}\|A\|B)$。

协议可不增加交互生成多重共享会话密钥：

$$K_1=H(g^{xy}\|A\|B),\cdots,K_m=H(g^{xy}\|K_{m-1}\|A\|B)$$

定理 3 DDH假设下，$\mathrm{SKP_{AM}}$协议在AM中是会话密钥安全的。

证明 为方便，本文只考虑两方的情况(以下证明同)。根据AM的定义，当两个未被共同攻陷的参与者A和B都完成了协议时，它们都得到了未被篡改的a和b，$r=r'=g^{xy}$。因此，它们建立了相同的会话密钥$K=H(g^{xy}\|A\|B)$。g^x和 g^y与会话标示s绑定在一起。协议满足了定义1中的性质1。

设存在一个密钥交换协议对手Adv在AM中有不可忽略的优势δ猜中b，则可以构造一个算法D能够以不可忽略地优势区分$Q_0=\{p,g,g^y,g^x,g^y,g^{xy}\}$和$Q_1=\{p,g,g^x,g^y,g^z\}$。令$D$的输入为$(p,g,a^*,b^*,c^*)$，它们为$Q_0$和$Q_1$的概率均为0.5。算法$D$使用Adv作为子过程。算法$D$描述如下：

(1) 选择$r \xleftarrow{R} \{1,2,\cdots,k\}$；

(2) 当参与者被攻陷或者某个会话暴露时，D把参与者或会话的信息交给Adv；

(3) 当第r个会话(A,s,a^*)被激活时，D让A把(A,s,a^*)发送给B；当B收到消息时，D让B把消息(B,s,b^*)发送给A；

(4) 如果会话(A,B,s)被选中进行测试会话查询，则D把c^*发送给Adv；

(5) 如果第r个会话暴露了，或Adv选择其他的会话作为测试会话，则D输出$b \xleftarrow{R} \{0,1\}$，然后停止；如果Adv停止且输出b，则D停止，输出与Adv相同的b。

可以看出，D所激发的Adv的运行和Adv对抗协议的正常运行是一致的。

当A选中第r个会话作为测试会话时，A相应得到的是r^*。如果D输入的是Q_0，则响应是真实的会话密钥，如果D的输入来自Q_1，则响应是一个随机数。在这种情况下，A猜中的概率是$0.5+\delta$，其中δ是概率不可忽略的。通过输出与A相同的b，D猜中的概率也为0.5+δ，其中δ是概率不可忽略的。

当A没选中会话r时，D输出一个随机数b，在这情况下，D猜中Q_0和Q_1的概率为0.5。

选中r的概率是$1/r$，没选中r的概率是$1-1/r$，故D猜中的概率$p=(0.5+\delta)\times 1/r+0.5\times(1-1/r)=0.5+\delta/r$，其中$\delta/r$是不可忽略的，这与DDH假设相悖，所以协议满足定义1的性质(2)。

故协议$\mathrm{SKP_{AM}}$在AM中是会话密钥安全的。

2.2 构造消息传输认证器λ_{PMAC}

参数设置：发起方为A，响应方为B，待传递消息为m，其余参数p、q、g设置同$\mathrm{SKP_{AM}}$协议。E_P是安全公钥加密算法；MAC是安全认证码算法。

(1) A随机选择$x \in Z_p^*$，发送$(m,C_A=E_{P_B}(g^x))$给B，输出A send message m to B；

(2) B收到消息后，解密g^x，获得随机选择$y \in Z_p^*$，发送$(m,C_B=E_{P_A}(g^y))$给A；

(3) A收到消息后，经解密运算得到g^y，发送$(m,C=\mathrm{MAC}_N(m,B))$给$B$，$N=g^{xy}$；

(4) B收到该消息后，验证MAC值，如果接受，输出B Receive m from A。

定理 4 假设公钥加密算法E_P是理想密码模型，且MAC是安全的认证码算法，则消息传输认证

器λ_{PMAC}可以模仿UM环境下的消息传输协议。

证明　设Adv_2是与λ_{PMAC}交互的UM对手，构造一个AM对手Adv_1使得两个协议的全局输出在计算上是不可区分的。Adv_2在UM中与运行λ_{PMAC}的参与者A'、B'进行交互，Adv_1在AM中与A、B交互。Adv_1按照以下规则进行：

(1) 当Adv_2激活A'并把消息m发送给B'时，Adv_1在AM中激活A发送消息m给B；

(2) Adv_2与A'、B'继续进行交互；

(3) 当B'输出B' Receive m from A'时，Adv_1使用来自A的消息m激活B；

(4) 当Adv_2攻破UM中的某个参与者时，A攻破AM中对应的参与者；

(5) Adv_1输出Adv_2输出的任何信息。

显然，如果模仿成功，Adv_1和Adv_2的输出统计是完全相同的。

设β表示如下事件：B' Receive m from A'，同时A'未被攻破，而(m,A,B)不在当前待传递消息集合中。如果β发生则表明Adv_2成功伪造了一个新的MAC值，因此，需证明β发生的概率可忽略。

在理想密码模型中，E_P是一个随机置换，因此Adv_2在不询问oracle E_P的情形下，也能导致β事件的发生，但除了在线穷举，不可能得到(m,C_B)的任何信息。因此，本文只考虑必须询问随机预言的情形下，事件β的发生概率是否可忽略。

假设β发生的概率是δ。以Adv_2为子程序构造一个MAC伪造者F。记UM中的通信双方为A和B；敌手为Adv_2。在事件β以概率δ发生的条件下，设L是Adv_2在运行协议过程中传递的消息总数，则在至多L次询问相应MAC oracle MAC_N条件下，MAC伪造者F的成功概率就是δ/r。

伪造者F定义为：其输入是N^*、x、$C_A=E_{P\_B}(g^x)$、$C_B=E_{P\_A}(g^y)$、$C=\mathrm{MAC}_{N^*}(m,B)$和$N^*=g^{xy}$ (N^*是未知的)。F拥有oracle E_P和以N^*为验证密钥的MAC Oracle MAC_{N^*}。F将模仿用户A和B与敌手Adv_2交互运行协议。设m^*是用以激活B的全部消息中随机选定的一个消息。如果模仿过程中A被收买，则F宣告失败，放弃模仿。

(1) 当B被敌手用消息(m^*,C_A)激活，则F用(m^*,C_B)回答，C_B恰好就是F的输入密文；

(2) 当A被来自B的消息(m^*,C_B)激活，且$m\neq m^*$，则F随机选取N，回答$C=\mathrm{MAC}_N(m)$；

(3) 如果C_A被询问过，则F询问MAC oracle MAC_{N^*}作为回答。而如果$m=m^*$，F放弃模仿；

(4) 如果敌手Adv_2使用来自A的消息(m^*,C_A)激活B，则F输出(m^*,C)。

在F不放弃模仿的情形下，敌手Adv_2与F的交互过程与Adv_2与UM用户交互的统计分布相同。

设β^*表示如下事件：在的模仿中，用户A被假冒，且对应的假冒消息是m^*。由于m^*是随机选取的，而且β^*事件和放弃模仿事件不会同时发生，因此事件β^*的发生概率为δ/L。

当β^*发生时，m^*就是假冒消息，B最后接收到的消息是一个合法的MAC值(对应的验证密钥是N^*)，而且A从未生成过对应消息的MAC值，F以概率δ/L成功伪造一个新消息的MAC值，δ/L是概率不可忽略的，与“MAC算法是安全的”这一假设矛盾。

综上所述，如果公钥加密算法E_p是理想密码模型，且MAC是安全的认证码算法，则消息传输认证器λ_{PMAC}可模仿UM环境下的消息传输协议。

2.3　构造UM下会话密钥安全的认证协议$\mathbf{SKP}_{\mathbf{UM}}$

参数设置：设p、q为素数，$q|p-1$，g是群Z_p^*中阶为q的元素；s为标示符；发起方为US_1；响应方为US_2；$H:\{0,1\}^{\infty}\rightarrow\{0,1\}^n$为安全Hash函数；$E_P$为安全公钥加密算法；MAC是安全认证码算法。

(1) US_1随机选$x\in Z_p^*$、$a=g^x$，发送$E_{P_\mathrm{us}_2}(\mathrm{us}_1,\mathrm{us}_2,s,a)$消息给$\mathrm{US}_2$；

(2) US_2收到消息后，解密，获得a，随机选择$y\in Z_p^*$、$b=g^y$、$r=a^y=g^{xy}$、$N=r$，删除y，把消息$(E_{P_\mathrm{us}_1}(\mathrm{us}_1,\mathrm{us}_2,s,b),\mathrm{MAC}_N(b))$发送给$\mathrm{US}_1$，输出会话密钥$K=H(g^{xy}||\mathrm{us}_1||\mathrm{us}_2)$。

(3) US_1收到消息$(E_{P_\mathrm{us}_1}(\mathrm{us}_1,\mathrm{us}_2,s,b),\mathrm{MAC}_N(b))$后，解密，计算$r'=b^x=g^{xy}$，验证验证码，如果接受，则生成会话密钥$K=H(g^{xy}||\mathrm{us}_1||\mathrm{us}_2)$，删除$x$。

至此，用户间的认证和密钥协商完成[6]。根据定理2～4，易得$\mathrm{SKP}_{\mathrm{UM}}$协议在UM下是安全的。

密钥更新流程如下：

(1) US_1和US_2调用协议$\mathrm{SKP}_{\mathrm{UM}}$，生成共享会话密钥$K_1=H(g^{xy}||\mathrm{us}_1||\mathrm{us}_2)$和$K_2=H(g^{xy}||K_1||\mathrm{us}_1||\mathrm{us}_2)$；

(2) US_1随机选取$R\xleftarrow{R}\{0,1\}^k$，传送消息$(m=E_{K_1}(R),\mathrm{MAC}_{k_2}(m))$给响应方$B$，计算$K_{\mathrm{New}}=H(g^{xy}||R||\mathrm{us}_1||\mathrm{us}_2)$；

(3) US_2收到消息$(m,\mathrm{MAC}_{k_2}(m))$后，验证验证码，如果接受，解密，计算$K_{\mathrm{New}}=H(g^{xy}||R||\mathrm{us}_1||\mathrm{us}_2)$，则双方都获得了新的密钥。

根据定理4可知密钥更新过程是安全的。

3 安全与性能

3.1 安全分析

双向实体认证：US_1和US_2通过发送消息$E_{P_us_2}(us_1,us_2,s,a)$、$E_{P_us_1}(us_1,us_2,s,b)$和验证码$MAC_N(b)$来实现。由于$E_{P_us_1}$只有$US_1$可以解密，$E_{P_us_2}$只有$US_2$可以解密，且由于$N=g^{xy}$只有$US_1$和$US_2$可以生成，故$MAC_N(b)$也只能由$US_1$和$US_2$进行生成和验证；从而实现了用户间的双向实体认证。

密钥协商：US_1和US_2之间的会话密钥是由US_1和US_2分别给出相关的安全参数产生的。g^{xy}和g^{y}都以公钥加密传输，基于CDH假设，g^{xy}只有US_1和US_2间共享，故$K=H(g^{xy}||us_1||us_2)$也只有US_1和US_2才能获得。消息$MAC_N(b)$在确认双方身份的同时完成会话密钥的一致性确认。

密钥更新：利用协议产生的多重会话密钥，利用消息$(m=E_{k_1}(R),\mathrm{MAC}_{k_2}(m))$完成会话密钥的更新。$H$是伪随机函数，因此密钥数据的统计结构被有效“遮蔽”，且由于攻击者不可能得到任何新旧密钥的关联等式，故双重字典[12]攻击也不成立。

完美的前向保密性：在密钥的生成和更新过程中，攻击者即使掌握了双方的当前会话密钥，由于不能获得g^{xy}；且由于密钥更新时新旧密钥不存在任何关联等式，故具有完美的前向保密性。

3.2 性能分析

通信性能：协议在完成双向身份认证的同时实现会话密钥的协商和确认，发起方和响应方仅交互2轮，而密钥更新只需进行1轮，交互即可实现，对比已有各种认证协议，通信开销大幅减少。

计算量分析：在整个身份认证和密钥协商过程中，发起方和响应方都仅需进行1次基于公钥的加密和解密运算；在密钥更新的过程中发起方仅进行1次对称加密运算，响应方则只需进行1次对称解密运算。与现有各种认证协议相比有较快的实现速度。

4 结 束 语

本文基于CK模型提出了一种新的可证明安全的快速认证协议，该协议实现了CK模型下可证明安全的快速身份认证、密钥协商和密钥更新，且具有双向实体认证、完美的向前保密性等安全属性，满足了身份认证和密钥协商的安全需求。该认证协议在执行中仅需进行2轮交互即可完成认证和密钥协商，1轮交互即可实现密钥更新，通信开销小，计算量较低，为用户间的相互认证提供了一种高效的解决方案。

参 考 文 献

[1] YANG F Y, JAN J K. An enhanced and secure protocol for authenticated key exchange[DB/OL]. [2004-10-21]. http://eprint .iacr.org/2004/270.

[2] YIN Shing TIN, TERRY BOYD C. Provably secure mobile key exchange: applying the canetti-krawczyk approach[C]// ACISP 2003. Berlin, Heidelberg: Springer-Verlag, 2003: 166-179.

[3] 冯登国, 陈伟东. 基于口令的安全协议的模块化设计与分析[J]. 中国科学E辑, 2007, 37(2): 223-237.
FENG Deng-guo, CHEN Wei-dong. Password based security protocol design and analysis[J]. Science in China(Series E: Information Sciences), 2007, 37(2): 223-237.

[4] BELLARE M, ROGAWAY P. Entity authentication and key distribution[C]//Advances in Cryptology-CRYPTO ’93. Berlin, Heidelberg: Springer-Verlag, 1994, 773: 232-249.

[5] RAIMONDO M D, GENNARO R. Provably secure threshold password-authenticated key exchange[C]// Proceedings of the Advances in Cryptology-Eurocrypt 2003. LNCS 2656, Berlin, Heidelberg: Springer-Verlag, 2003: 507-523.

[6] 谭示崇, 张 宁, 王育民. 新的口令认证密钥协商协议[J]. 电子科技大学学报, 2008, 37(1): 17-19.
TAN Shi-chong,ZHANG Ning,WANG Yu-min. A new password-based authenticated key agreement protocol[J]. Journal of University of Electronic Science and Technology of China, 2008, 37(1): 17-19.

[7] JIANG Yi, SHI Hao-shan. A cluster-based random key revocation protocol for wireless sensor networks[J]. Journal of Electronic Science and Technology of China, 2008, 6(1): 10-15.

[8] CANETTI R, KRAWCZYK H. Analysis of key-exchange protocol and their use for building secure channel[C]// Proceedings of the Euro-crypt 01. Denmark: [s.n.], 2001: 453-474.

[9] BELLARE M, CANETTI R, KRAWCZYK H. A modular approach to the design and analysis of authentication and key exchange protocols[C]//Proceeding of the 30th Annual Symposium on the Theory of Computing. New York: ACM Press, 1998: 419-428.

[10] MICALI S, ROGAWAY p. Secure computation[C]// Proceeding of the Advances in Cryptology-Crypto ’91: LNCS 576. Berlin, Heidelberg: Springer-Verlag, 1991: 392-404.

[11] CANETTI R, GOLDREICH O, HALEVI S. The random oracle methodology, revisited[J]. Journal of the ACM, 2004, 51(4): 557-594.

[12] WANG C I, FAN C I, GUAN D J. Cryptanalysis on Chang-Yang-Hwang protected password change protocol[DB/OL]. [2006-01-12]. http://eprint. iacr. org/2005/182.

编 辑 熊思亮