一个可抵抗临时指数泄露的密钥协商协议形式化安全模型

陶文君 胡 斌
(解放军信息工程大学 郑州 450004)

摘 要 从临时指数泄露这一新的假设出发,分析了eCK模型下临时指数泄露可能造成的安全隐患,提出了可抵抗临时指数泄露的新安全属性,建立了攻击者具有更强能力的新形式化安全模型。在该模型下,给出了一个可证明安全的HCMQV密钥协商协议,该协议在CMQV的基础上对参数 e 的生成方式做了自然的修改并增加了保密性,以有效减少协议执行中杂凑的次数和抵抗反射攻击。为了证明协议的安全性,没有沿用HMQV协议证明签名机制不可伪造性的方法,而是通过构造区分器将新协议的安全性紧凑地归约到DDH问题上。事实证明,设计临时指数可泄露的安全密钥协商协议是可行的。

关键词 CMQV,eCK,形式化安全模型,可证明安全性
中图法分类号 TP309 **文献标识码** A

Formal Security Model Resisting Session Exponential Reveal for Key Agreement Protocol

TAO Wen-jun HU Bin
(Information Engineering University, Zhengzhou 450004, China)

Abstract Based on the assumption of ephemeral exponential leakage in eCK model, this paper analyzed the effect of this hidden trouble and built a new formal security model in which a much stronger adversary can be resisted and also a new security attribute can be satisfied. Futher more, a provable secure key agreement protocol-HCMQV was designed in this new model. The protocol modifies the generation function of e in a natural way and makes it in secrecy. The method reduces the times of HASH and also the reflect attack can be avoided. In order to prove the security of HCMQV, we did not prove the unforgeability for the signature scheme like HMQV, but a distinguisher was constructed to reduce the security of protocol to DDH assumption tightly. Actually, designing a secure key agreement protocol in which ephemeral exponential can be leaked is possible.

Keywords CMQV, eCK, Formal security model, Provable security

1 引言

2007年LaMacchia等人在CK模型[1]的基础上,扩展得到了一个新的两方密钥协商协议形式化安全模型——eCK[2],该模型相比改进的CK模型[3]具有更强的安全性,是目前为止公认的安全性最强的安全模型[4]。在该模型下攻击者被赋予两种新的攻击能力即长期密钥查询(Long-Term Key Reveal)和临时密钥查询(Ephemeral Key Reveal)。若令 $\overline{A}=g^a$,$\overline{B}=g^b$ 分别表示身份为 A,B 的实体所拥有的一对公私钥,则攻击者可以通过Long-Term Key Reveal(A)查询得到实体A公钥所对应的长期私钥 a,或通过Ephemeral Key Reveal(A)查询得到实体 A 在会话中产生的临时密钥 $\tilde{x}$。在考察eCK模型攻击者能力时我们发现:该模型明确定义攻击者不能通过查询得到 $H_1(\tilde{x},a)$ 的任何信息,这意味着一个强假设:攻击者不能得到密钥协商协议(基于DH协议的)交互消息的指数上的任何信息!在本文中我们称之为临时指数不可泄露。

eCK模型对临时指数的产生与运算做了较详细的描述:协议执行过程中产生的长期密钥和临时密钥被存储在不同安全级别的存储器中,当协议需要计算临时指数 $H_1(\tilde{x},a)$ 时,分别调用 $\tilde{x}$ 和 a,且在本次计算完成后立即彻底删除该临时指数,当下次需要的时候再重新进行计算。这样做的优点是可以在一定程度上避免临时指数的泄露,但缺点也显而易见,就是协议的执行效率会受到一定的影响。为保证效率,$H_1(\tilde{x},a)$ 通常并不能太长,而随着旁路攻击等新技术的不断发展,攻击者往往具有超出我们预期的攻击能力,因此临时指数的安全性也并不一定能得到保证,所以对临时指数 $H_1(\tilde{x},a)$ 泄露时两方密钥协商协议的安全性进行研究十分必要。

2010年,Cheng等人将eCK模型扩展为适用于三方的强形式化安全模型[5]。最近文献[6-8]分别给出了eCK安全的认证密钥协议,但模型本身的安全性并没有再得到扩展。2011年,Fujioka等人提出了抗临时秘密信息泄露的密钥协商协议[9],但未考虑临时指数泄露的情况。在本文的研究中,我们首先分析了临时指数泄露对eCK安全密钥协商协议安

到稿日期:2013-01-22 返修日期:2013-05-22 本文受国家自然科学基金(61272488,61272041,61202491)资助。
陶文君(1985—),男,硕士生,主要研究方向为安全协议,E-mail:taowenjun515@163.com;胡 斌(1971—),男,博士,教授,博士生导师,主要研究方向为信息安全。

全性的影响，再进一步尝试解除 eCK 模型中临时指数不可泄露的限定条件，针对攻击能力大幅提高的攻击者，建立新的安全强度更高的两方密钥协商协议形式化安全模型，该模型满足一种新的安全属性——临时指数安全。在新模型下，我们基于 CMQV 协议[10]设计了一个随机预言模型[11]下可证明安全的 HCMQV 协议，将原协议的公开参数 d、e 简化为一个参数 e，并对 e 进行了一定的加密处理，使得新的协议可以有效地抵抗反射攻击和临时指数泄露。最后我们在新模型下将该协议的安全性归约到了 DDH 问题上。

2 临时指数泄露与新的安全属性

eCK 模型明确定义了攻击者可以得到某次会话的长期私钥 a 或者临时私钥 $\tilde{x}$，但不能同时得到 a、$\tilde{x}$。但是在现有的攻击条件下，攻击者可能通过某些手段得到关于 a、x 的一个预言 $H_1(\tilde{x},a)$，我们称之为临时指数。对于 eCK 安全模型而言，临时指数的泄露可能会造成会话密钥的不安全。为了验证临时指数泄露对会话密钥安全性的影响，在本节中我们对两个经典的 eCK 模型下安全的两方密钥协商协议 NAXOS 和 CMQV 进行了简要分析。为了描述临时指数 $H_1(\tilde{x},a)$ 泄露的情况，我们形式化地定义攻击者可以通过 Session Exponential Reveal(A) 查询得到该临时指数，即对于 NAXOS 和 CMQV 协议来说攻击者可以得到 $H_1(\tilde{x},a)$ 或 $H_1(\tilde{y},b)$。值得注意的是，由于 H_1 是随机 Oracle，攻击者即使通过此查询获得临时指数 $H_1(\tilde{x},a)$，也不能得到 $\tilde{x}$、a 的任何信息。

我们知道，对于会话密钥 $K=H_2(\sigma_1,\sigma_2,\cdots,A,B)$，如果 H_2 是随机 Oracle，则会话密钥 K 的安全性完全依赖于五元组$(\sigma_1,\sigma_2,\cdots,A,B)$的安全性。为了更好地分析，我们给出了 Reveal 查询的一个更强定义：当攻击者对某个已完成的会话进行 Reveal 查询时，此 Oracle 返回给攻击者会话密钥杂凑前的所有相关信息，例如在 NAXOS 协议中该查询返回给攻击者会话密钥的五元组$(Y^a,\overline{B}^{H_1(\tilde{x},a)},Y^{H_1(\tilde{x},a)},A,B)=(\overline{A}^{H_1(\tilde{y},b)},X^b,X^{H_1(\tilde{y},b)},A,B)$。需要说明的是：这样的修改虽然将大幅加强攻击者的能力，但并不意味着攻击者可以由 $K=H_2(\sigma_1,\sigma_2,\cdots,A,B)$计算出$(\sigma_1,\sigma_2,\cdots,A,B)$的任何信息，而只是对攻击者获得会话密钥信息的更强一步定义。为了说明对 Reveal 查询修改的合理性，我们将在第 3 节中对这类攻击者建立新的形式化安全模型并在此模型下设计安全协议。下面介绍利用攻击者的上述能力对 NAXOS 协议的攻击。

2.1 临时指数泄露时 NAXOS 的安全性

攻击 1 A,B 的一个会话实例 $\pi^i_{A,B}$生成会话密钥 $K_A=H_2(Y^a,\overline{B}^{H_1(\tilde{x},a)},Y^{H_1(\tilde{x},a)},A,B)$，攻击者通过 Reveal 查询得到$(Y^a,\overline{B}^{H_1(\tilde{x},a)},Y^{H_1(\tilde{x},a)},A,B)$，即可得到 Y^a。现在实体 A 试图与 B 发起一个新的会话，此会话也是攻击者要攻击的测试会话：A 发送 $X'=g^{H(\tilde{x}',a)}$ 给 B，攻击者 E 截获此消息，冒充 B 重放会话 $\pi^i_{A,B}$中的消息 $Y=g^{H_1(\tilde{y},b)}$ 给 A，并通过 Session Exponential Reveal 查询得到 A 的临时指数 $H_1(\tilde{x}',a)$。此时易发现，由于消息 Y 没有改变，攻击者可以计算新的会话密钥 $K_A'=H_2(Y^a,\overline{B}^{H_1(\tilde{x}',a)},Y^{H_1(\tilde{x}',a)},A,B)$，从而造成会话密钥不安全。在上述攻击中，攻击者利用了会话密钥的相关性和临时指数的信息泄露。

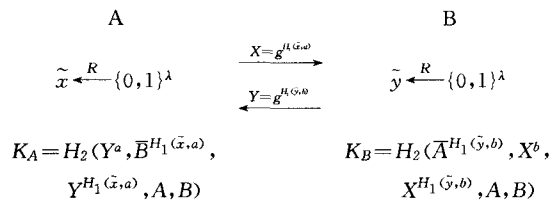

图 1 NAXOS 协议

攻击 2 临时指数泄露时该协议还容易受到反射攻击。即当攻击者冒充 B 发送给 A 的消息 $Y=X$ 时，攻击者可以利用已知的 $H_1(\tilde{x},a)$直接计算会话密钥。

2.2 临时指数泄露时 CMQV 的安全性

与对 NAXOS 的攻击类似，在 CMQV 协议中我们假定攻击者可以通过 Session Exponential Reveal 和 Reveal 查询得到 $\pi^i_{A,B}$的 $H_1(\tilde{x},a)$和 $\sigma_A=(Y\overline{B}^e)^{H_1(\tilde{x},a)+da}$，并计算$(Y\overline{B}^e)^a=(\sigma_A/(Y\overline{B}^e)^{H_1(\tilde{x},a)})^{1/d}$。现在攻击者对实体 A 新发起一个会话进行攻击：A 发送 $X'=g^{H(\tilde{x}',a)}$ 给 B，攻击者 E 冒充 B 重放会话 $\pi^i_{A,B}$中的消息 Y，同样容易计算 $\sigma_A'=(Y\overline{B}^e)^{H_1(\tilde{x}',a)+d'a}=(Y\overline{B}^e)^{H_1(\tilde{x}',a)}\cdot((Y\overline{B}^e)^a)^{d'}$。此外该协议同样容易受到反射攻击。

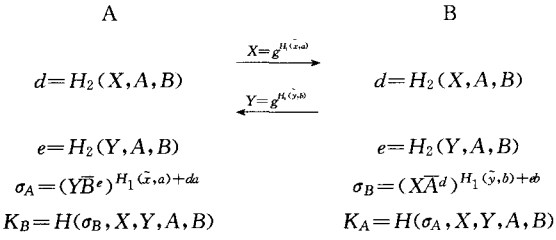

图 2 CMQV 协议

通过对上述两协议的分析发现，第一种攻击能够成功的原因是当攻击者冒充某一方重放消息时会话密钥中一部分信息并未改变，而改变的部分信息是可以利用 $H_1(\tilde{x},a)$或 $H_1(\tilde{y},b)$直接计算的。因此自然想到，能否设计一种新的密钥生成方式，使得即使临时指数泄露仍然能保证会话密钥的安全呢？由于 CMQV 协议有更高的效率，我们尝试对此协议进行修改以避免上述的攻击方法。在对 CMQV 的攻击中，$(Y\overline{B}^e)^a$ 是未被改变的部分信息，其中 Y、B 是公开信息，a 是固定的长期私钥，因此可改变的部分只有 e，如果 e 与消息 X 相关则可以解决上述问题，因此我们可以将 CMQV 协议的 e 修改为：$e=H_2(X,Y,A,B)$。由于 e 随 X 的变化而变化，因而此前的攻击不再能成功。

但我们随后发现，即使令 $e=H_2(X,Y,A,B)$，协议仍然不安全。这是因为 $H_1(\tilde{x},a)$的泄露会使协议非常容易受到反射攻击，即如果攻击者将 A 发送给 B 的消息 $X=g^{H(\tilde{x},a)}$ 作为 Y 再重新发送给 A，那么攻击者可以在已知 $H_1(\tilde{x},a)$的情况下利用已知的会话密钥计算测试会话的会话密钥。要避免这种情况的发生最直接的办法是对参数 e 进行一定的加密，使得攻击者难以计算 e 的信息，从而无法利用会话密钥之间的相关性。因此 e 在满足随 X、Y 动态性变化的同时也必须满足保密性，而 e 的生成参数中必须具有双方都可计算的秘密值。由于攻击者已知 $H_1(\tilde{x},a)$的能力，因此利用 X、Y 这样的临时公钥无法完成对 e 的加密处理，所以我们考虑令 $e=H_2(g^{ab},X,Y,A,B)$来达到保密性。这样做能够有效的原因在于无论攻击者已知 a 还是 b 都无法在新模型中保证会话新

鲜性的前提下完成反射攻击。因此我们认为对 e 的修改是合理的。

2.3 新的安全属性——临时指数安全

我们称可以抵抗临时指数泄露的协议满足一种新的安全属性——临时指数安全。这一性质与前向安全有些相似。前向安全是指攻击者即使知道某一方的长期密钥也不能恢复此前会话的会话密钥，而临时指数安全是指攻击者即使已知某一方的临时指数也不能恢复该会话的会话密钥。就实际意义而言，由于临时指数的长度直接决定协议的执行效率，因此通常该指数的长度并不能太长。正因为如此，只要临时指数可能泄露，则设计满足上述安全属性的新协议就十分必要。由于攻击者能力的大幅提高和新安全属性的提出，我们很有必要建立新的更强的安全模型，同时我们发现，本文第 3 节中给出的 HCMQV 协议在新模型下是可证明安全的。

3 安全模型

3.1 攻击者能力

在第 2 节中，我们实际上给出了一个新的攻击者模型，该攻击者除了具有 eCK 模型下攻击者的能力以外，还可以获得任意会话实例中某一方的临时指数，且可以查询除测试会话以外任意会话的会话密钥的生成元组。对于具有这种能力的攻击者，eCK 模型下可证明安全的协议将不再安全。

在本文所述的新模型中，称协议某一方的一次执行为一个会话实例。协议的参与方可能是协议的发起方也可能是协议的回应方，令 $role\in\{I,R\}$ 表示攻击者的角色，I 表示其为协议的发起方，R 则表示回应方。我们称协议执行中与实体交互的另一方为 Partner。参与协议的实体身份用 A、B 表示。以实体 A 为例，它拥有相应的公私钥对 $(\overline{A},a)$，其中 $\overline{A}=g^a$。为了描述一个会话实例，我们沿用 eCK 模型中的方法，用会话标识符 $sid=(role,ID,ID',m_1,m_2\cdots)$ 来描述一次会话，其中 role 是该方扮演的角色，ID 为其对应的身份，ID′是另一方的身份，$m_1,m_2,\cdots$ 是两方交互的消息内容。如果存在另一个已完成的会话有标识符 $sid'=(\overline{role},ID',ID,m_1,m_2\cdots)$，则称它们是匹配会话，如果两个诚实实体间交互的消息被攻击者修改或截断，则称匹配会话不存在。该模型中攻击者 E 可以视作一个拥有有限多个 Oracle 的概率图灵机。攻击者可以完全控制实体间的消息交互，这意味着攻击者可以修改、替换、转发、重放、截断以及延迟任意两个实体之间的传递的消息。此外攻击者还可以获得一些会话的特定秘密信息，我们将这种攻击者形式化描述如下：

Send(A,B,M)：攻击者 E 冒充 B 发送消息 M 给 A，会话 Oracle 返回给攻击者对消息 M 的执行结果。该查询用于模拟攻击者对 A、B 之间交互的主动攻击。$Send(A,B,null)$ 表示攻击者让 A、B 之间发起一个新的会话实例。

Reveal(sid)：与 CK、eCK 模型稍有不同，该查询直接返回给攻击者会话密钥的生成元组，即会话密钥 hash 前的内容。

Long-Term Key Reveal(A)：返回给攻击者实体 A 的长期私钥 a。

Ephemeral Key Reveal(A)：与 eCK 模型中定义相同，返回给攻击者实体 A 的临时密钥 $\tilde{x}$，但不包括临时指数 $H(\tilde{x},a)$。

Session Exponential Reveal(A)：返回给攻击者实体 A 交互(不含计算)过程中产生的临时指数 $H(\tilde{x},a)$。

Test(sid)：攻击者只能对已完成的、新鲜的会话进行一次 Test 查询。挑战者随机掷币 $b\in\{0,1\}$，如果 $b=1$ 返回给攻击者 Reveal(sid)，否则 $b=0$ 返回给攻击者会话密钥空间中的随机值。攻击者根据 Oracle 返回的结果输出一个关于 b 的猜测值 b'。令 $\Pr[b=b']$ 表示攻击者猜测成功的概率，为描述攻击者在攻击实验中成功的情况，定义攻击者的优势为 $Adv_{sid}^{E}=2\Pr[b=b']-1$。

我们称具有上述能力的攻击者为 H-AKE 敌手。

3.2 会话新鲜性

会话的新鲜性用于限制攻击者的某些攻击情况，在这些情况下攻击者可以直接计算两方协商的会话密钥，因此在安全性定义中必须排除掉。但是这些限制也不能太严格，这样才可以保证攻击者能力的最大化。对于两方协议来说，一方会话的新鲜性在一定程度上依赖于攻击者对另一方会话的信息获取程度，因此在定义会话新鲜性时我们需要考虑该会话的匹配会话。

正如上文中所述，当攻击者只能对两个诚实实体间完成的会话进行被动攻击时，我们认为匹配会话存在，相反在遇到攻击者的主动攻击时，则认为匹配会话不存在，因此会话新鲜性的定义需要综合考虑以上两种情况。在建立此模型时，我们先给出了攻击者在已知长期密钥、临时密钥和临时指数这些信息时的新鲜性情况，如表 1 和表 2 所列，然后我们将通过具体协议的安全性证明来说明此新鲜性定义的合理性和有效性。由于新的模型是在 eCK 的基础上扩展而来的，因此当攻击者能力与 eCK 模型中攻击者能力完全相同时，两者的新鲜性将完全相同。

表 1 和表 2 中的灰色部分可以看作是 eCK 模型下会话新鲜性的情况，表格整体表示在新模型下会话新鲜性的情况。容易看出新模型较大地扩展了原有的安全模型。在协议的证明中，如果新协议至少是 eCK 安全的，则我们不需要对表格灰色的部分进行证明，因为如果 eCK 安全，则意味着灰色部分安全。由于表 1 和表 2 都是对称的，我们仅需要考虑灰色部分以外出现“√”的情况，此时攻击者往往具有较强的攻击能力，而且测试会话也仍然是新鲜的。

表 1 匹配会话存在

	$H(\tilde{x},a)$	$H(\tilde{y},b)$	a	$\tilde{x}$	b	$\tilde{y}$
$H(\tilde{x},a)$	√	×	×	√	√	√
$H(\tilde{y},b)$	×	√	√	√	×	√
a	×	√				
$\tilde{x}$	√	√				
b	√	×				
$\tilde{y}$	√	√				

注：√表示攻击者不能直接计算会话密钥；×表示攻击者可以直接计算会话密钥

表 2 匹配会话不存在

	$H(\tilde{x},a)$	$H(\tilde{y},b)$	a	$\tilde{x}$	b	$\tilde{y}$
$H(\tilde{x},a)$	×	×	×	×	×	×
$H(\tilde{y},b)$	×	√	√	√	×	√
a	×	√				
$\tilde{x}$	×	√				
b	×	×				
$\tilde{y}$	×	√				

注：√表示攻击者不能直接计算会话密钥；×表示攻击者可以直接计算会话密钥

定义 1 如果会话 sid 符合下面任何一种情况，则称其是

不新鲜的，反之则称该会话是新鲜的。

(1)该会话 sid 或其匹配会话 sid' 被进行过 Reveal 查询

(2)匹配会话 sid' 存在时：

攻击者同时得到 $a,\tilde{x}$ 或 $b,\tilde{y}$

攻击者同时得到 $a,H(\tilde{x},a)$ 或 $b,H(\tilde{y},b)$

攻击者同时得到 $H(\tilde{x},a)$ 和 $H(\tilde{y},b)$

(3)匹配会话 sid' 不存在：

攻击者得到 b 或 $H(\tilde{x},a)$

攻击者同时得到 $a,\tilde{x}$

3.3 安全性定义

为了描述协议的安全性，我们设计了一个安全实验：攻击者 E 首先选择协议 P 的一个已完成会话 sid，并利用具备的攻击能力对该会话进行查询。在实验过程中攻击者可以随时进行 Test 查询，此后攻击者可以继续进行攻击直到输出一个对比特 b 的猜测 b'。我们称攻击者在此实验中成功，如果在输出 b' 时该会话仍然是新鲜的，且攻击者的优势 $Adv_{sid}^{E}=2\Pr[b=b']-1$ 是不可忽略的。

定义 2 如果不存在多项式时间 H-AKE 攻击者使得上述实验成功，则称协议 P 是安全的。

4 HCMQV 协议与安全性证明

本节给出了一个对 CMQV 协议的改进版本 HCMQV 协议，其具体执行过程如图 3 所示。其中 $H_1:\{0,1\}^*\rightarrow Z_p$，$H_2:\{0,1\}^*\rightarrow\{0,1\}^{\lambda}$，$H:\{0,1\}^*\rightarrow\{0,1\}^k$ 均为随机 Oracle，λ,k 为安全参数。实体的长期私钥为 $a,b\in Z_p$，公钥为 $\overline{A}=g^a,\overline{B}=g^b$，临时私钥 $\tilde{x},\tilde{y}\in\{0,1\}^{\lambda}$。该协议与 CMQV 的唯一不同在于 e 的生成方式不同。我们知道 CMQV 协议是由 HMQV 协议[3]构造而成，因此协议 HCMQV 本质上仍然是利用了一种改进的 XCR 签名机制，我们称之为 HXCR 签名机制：

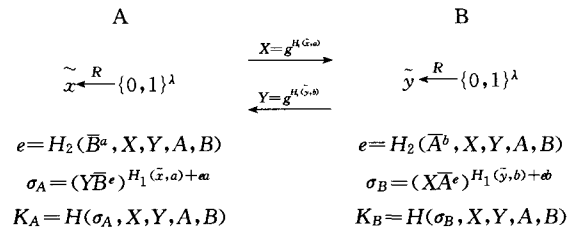

图 3 HCMQV 协议

HXCR 签名：实体 A 发送挑战 $X=g^{H_1(\tilde{x},a)}$ 给 B，实体 B 根据此挑战计算并输出一个签名对 (Y,σ)，其中 $Y=g^{H_1(\tilde{y},b)}$，$\sigma=(X\overline{A}^e)^{H_1(\tilde{y},b)+eb}$。$A$ 可以利用自己的私钥 a 和 $H_1(\tilde{x},a)$ 计算并验证相同的 σ 值。

在做本协议的安全性证明时，我们最初的想法是像 HMQV 协议一样，先证明签名机制 HXCR 的不可否认性。但随后我们发现，HMQV 利用了一个重要条件：如果攻击者可以对挑战 X 伪造一个签名对 (Y,σ) 和固定的值 d,e，那么对随机的 d',e'，攻击者仍然可以伪造该签名。文献对 XCR 的证明利用这一条件设计了一个重复性实验，并由此说明如果签名是可以伪造的，那么 CDH 问题是可解的。在 HXCR 签名机制中，上述条件明显不成立，这从本文第 2 节中给出的攻击实例便可以看出。因此我们进一步试想：如果攻击者在对挑战 X 伪造一个签名对 (Y,σ) 的情况下，能构造一个对挑战 X' 的伪造签名对 (Y,σ')，那么我们仍然能将 HXCR 签名的不可伪造性归约到 CDH 问题上。遗憾的是，我们随后发现，这种构造可能是困难问题。经过分析发现，将会话密钥的安全性归约到 CDH 问题上是具有一定难度的。因此我们尝试着降低困难问题的强度，即将会话密钥的安全性归约到判定性问题上。为了方便证明，我们通过一个安全实验将 DDH 问题重新做形式化的描述。

设 k 为安全参数，p,q 为素数。其中 q 的长度为 k 比特，且 $q|p-1$。g 是阶为 q 的群 Z_p^* 中的元素，攻击者随机选择 $x,y,z\in Z_P$，并进行一次随机掷币，设其结果为 b，如果 $b=1$，则令 $Z_1=g^{xy}$，否则令 $Z_0=g^z$。现有攻击算法 D 输入为 (g^x,g^y,Z_b)，攻击者根据输入信息输出对掷币结果的猜测值 b''，用 $\Pr[b''=b]$ 表示攻击者在实验中猜测成功的概率。若对任意多项式时间算法 D，都有攻击者的优势 $Adv_S^{DDH}=\Pr[b''=b]-1/2$ 是可忽略的，其中 $\Pr[b''=b]=\{g,g^x,g^y;Z_b;b\xleftarrow{R}\{0,1\},x,y,z\xleftarrow{R}Z_P\}$，则称 DDH 假设成立。

我们的证明思路是：首先利用反证法假设攻击者可以在 Test 查询中区分会话密钥和一个随机数。那么在攻击者进行所有能力范围内的查询后，也一定可以区分会话密钥和一个随机构造的“会话密钥”。进一步地，我们利用攻击者的这种区分能力构造一个区分器，来解决 DDH 问题，最后发现，如果最初的假设是正确的，则攻击者可以解决 DDH 问题，从而安全性得证。

定理 1 对 H-AKE 敌手，HCMQV 协议是安全的。

证明：我们首先证明匹配会话存在时攻击者能力最强的情况，即如果攻击者已知 $H_1(\tilde{x},a),b,\tilde{x}$ 成立，对于其它情况自然成立。首先我们尝试攻击者所有能力范围内的攻击，做如下实验：

Step1 Session Exponential Reveal(A)：攻击者对实体 A 进行临时指数查询，Oracle 返回给攻击者实体 A 当前会话的临时指数 $H_1(\tilde{x},a)$。

Step2 Ephemeral Key Reveal(A)：攻击者对实体 A 进行临时密钥查询，Oracle 返回给攻击者实体 A 当前会话的临时密钥 $\tilde{x}$。

Step3 Oracle($\tilde{x},R_a$)：攻击者随机选择 $R_a\in Z_P$，并连同 $\tilde{x}$ 一起发送给随机 OracleH_1，H_1 计算 $H_1(\tilde{x},R_a)$ 并判断 $H_1(\tilde{x},R_a)$ 是否等于 $H_1(\tilde{x},a)$，若相等，则攻击成功并终止实验，若不相等，则继续进行下一步。

Step4 Send(A,B,R_{Hb})：攻击者随机选择 $R_{Hb}\in Z_P$，计算 $Y'=g^{R_{Hb}}$ 并对测试会话进行 Send 查询，该 Oracle 判断是否有 $Y'=g^{R_{Hb}}$ 等于 $Y=g^{H_1(\tilde{y},b)}$，若相等，返回攻击成功并终止实验，若不相等，则继续进行下一步。

Step5 Long-Term Key Reveal(B)：攻击者对实体 B 进行长期私钥的查询，Oracle 返回给攻击者实体 B 当前会话的长期密钥 b。

Step6 Oracle(R_y,b)：攻击者随机选择 $R_y\in\{0,1\}^{\lambda}$，并连同 b 一起发送给随机 OracleH_1，H_1 计算 $H_1(R_y,b)$ 并返回该值给攻击者。

Step7 Send($A,B,H_1(R_y,b)$)：攻击者将 $H_1(R_y,b)$ 发送给测试会话进行 Send 查询，该 Oracle 计算并判断 $g^{H_1(R_y,b)}$ 是否等于 $g^{H_1(\tilde{y},b)}$，若相等则意味着执行结果为攻击者攻击成功并终止实验，若不相等则 Oracle 利用随机数计算并返回攻击者一个随机的会话密钥 $K'=H(g^{(H_1(\tilde{x},R_a)+e'a)(H_1(R_y,b)+e'b)}$，

$X,Y,A,B)$，其中 $e'=H_2(\overline{A}^b, g^{H_1(Ry,b)}, g^{H_1(\tilde{x},Ra)}, A, B)$。

若在上述攻击实验的第 3、4、7 步成功，则都可以使攻击者直接区分会话密钥和一个随机数。因为在第 3 步中如果成功，则攻击者可以直接得到实体 A 的长期私钥 a，进而计算会话密钥。在第 4 步中如果成功，则攻击者可以直接得到 $H_1(\tilde{y},b)$，同样泄露会话密钥。在第 7 步中成功，则攻击者可以直接得到实体 B 的临时私钥 $\tilde{y}$，而此时攻击者还可以得到其长期私钥 b，因此也可以计算会话密钥。下面我们分别计算这 3 种情况发生的概率。

Step 3 中攻击者成功的概率为 $q_{\sigma r}/p$，其中 $q_{\sigma r}$ 为 Oracle 查询次数。Step4 中攻击者成功的概率为 q_{se}^2/p，其中 q_{se} 为 Send 查询次数。Step7 中攻击者成功的概率为 $q_{se}^2/2^\lambda$。

对于安全的参数 p,λ，上述 3 个概率都是可忽略的。我们令 $D(K,K')$ 表示攻击者区分 K、K' 的最优算法，$Adv_S^{D(K,K')}$ 表示攻击者区分 K、K' 的优势，则攻击者在 Test 测试中的优势可以表示为：

$Adv_S^{HCMQV} \leqslant q_{\sigma r}/p + q_{se}^2/p + q_{se}^2/2^\lambda + Adv_S^{D(K,K')}$，如果攻击者在 Test 测试中的优势是不可忽略的，则容易得到 $Adv_S^{D(K,K')}$ 是不可忽略的。我们利用攻击者可以区分 K、K' 来构造一个 DDH solver。

我们知道，攻击者想区分会话密钥 K 和一个随机比特串只有两种方法：一种是密钥替换攻击，也就是攻击者能成功建立一个与测试会话不同的会话且这两个会话有相同的会话密钥。另一种方法是攻击者可以进行会话密钥的伪造，即可以计算一个五元组 (σ,X,Y,A,B) 使得 $H(\sigma,X,Y,A,B)=K$。对于密钥替换攻击，我们已知不同的会话一定有不同的五元组，则这类攻击成功意味着攻击者可以找到一个 H 函数的碰撞。根据协议假设 H 是一个随机 Oracle，碰撞发生的概率是可以忽略的。因此在证明中我们仅需要证明会话密钥的不可伪造性。生成会话密钥的五元组 (σ,X,Y,A,B) 中，X,Y,A,B 是公开信息，如果攻击者可以区分 K、K'，根据 Reveal 查询的新定义，那么攻击者必然可以区分 σ、σ'，我们只需要证明 σ 的不可区分性。利用反证法，假设 σ、σ' 是以不可忽略的概率可区分的，则攻击者能以不可忽略的优势输出 b' 使得 $b'=b$：

已知

$$\begin{aligned}\sigma &= g^{(H_1(\tilde{x},a)+ea)(H_1(\tilde{y},b)+eb)}\\ &= g^{H_1(\tilde{x},a)H_1(\tilde{y},b)+H_1(\tilde{x},a)eb+H_1(\tilde{y},b)ea+abe^2}\\ &= Y^{H_1(\tilde{x},a)} \cdot (\overline{B}^e)^{H_1(\tilde{x},a)} \cdot (\overline{A}^e)^{be} \cdot g^{H_1(\tilde{y},b)ea}\end{aligned}$$

在上述攻击实验中，攻击者已通过在 Step1、Step5 中的查询获得 $H_1(\overline{x},a)$ 和 b，分两种情况：

若 $b'=1$，则攻击者计算 $\gamma=(\sigma/Y^{H_1(\tilde{x},a)} \cdot (\overline{B}^e)^{H_1(\tilde{x},a)} \cdot (\overline{A}^e)^{be})^{1/e} = g^{H_1(\tilde{y},b)a}$

若 $b'=0$，则攻击者计算 $\gamma'=(\sigma'/g^{H_1(Ry,b)H_1(\tilde{x},Ra)} \cdot (\overline{B}^{e'})^{H_1(\tilde{x},Ra)} \cdot (\overline{A}^{e'})^{be'})^{1/e'} = g^{H_1(Ry,b)Ra}$

因为 R_y、R_a 是随机选择的，所以此时的 γ' 为随机数。现定义一个输入为 $(Y=g^{H_1(\tilde{y},a)}, \overline{A}=g^a, Z_b)$ 的 DDH solver。我们已知 $Z_1=g^{H_1(\tilde{y},b)a}$，$Z_0=g^r$（其中 r 是 Z_P 中随机选择的元素）。则对于 DDH solver 的输入 Z_b，攻击者能以不可忽略的优势输出一个对 Z_b 的判定结果 $b''=b'$，使得 $b''=1$ 时有 $Z_1=\gamma$，当 $b''=0$ 时有 $Z_1=\gamma'$，这明显与 DDH 假设相矛盾，因此在 Test 测试中攻击者的优势是可以忽略的。匹配会话存在的情况证毕。

当 *sid* 的匹配会话不存在时，意味着攻击者对 Partner 的消息进行修改。不妨假设攻击者可以对 $Y=g^{H_1(\tilde{y},b)}$ 进行修改，此时也意味着攻击者可能已知 $H_1(\tilde{y},b)$，通过对表 2 中新鲜性的观察可以发现攻击者最强的能力是已知 $H_1(\tilde{y},b)$，a，$\tilde{y}$。此时的安全性证明与刚才已知 $H_1(\tilde{x},a)$，b，$\overline{x}$ 基本相同。因此我们称 HCMQV 协议在新的安全模型下是安全的。

结束语 本文针对 eCK 模型中临时指数泄露的情况，提出了一个扩展的新模型。该模型较大地强化了攻击者的能力，并满足新的安全属性——临时指数安全。对于满足该属性的新协议，即使某一方的临时指数泄露，也不会影响会话密钥的安全性。这对两方密钥协商协议安全有着十分重要的意义。在本文给出的 HCMQV 协议中，我们对参数 e 的生成方式做了最自然的修改，减少了协议执行中杂凑的次数，且使该协议能有效地抵抗反射攻击。在安全性证明中我们没有沿用 HMQV 协议通过签名机制的安全性证明方法，而是通过构造区分器将新协议的安全性归约到 DDH 问题上。在下一步工作中，我们将尝试新的协议设计方法，努力使得攻击者即使在协议执行前可以获得 g^{ab} 的信息，也不能进行反射攻击。此外本文给出的 HCMQV 协议的安全性依赖于 DDH 问题，能否在新模型下给出安全性依赖于 CDH 问题的安全协议同样是我们将来研究的重要内容。

参 考 文 献

[1] Canetti R, Krawczyk H. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels[C]// Advances in Cryptology — EUROCRYPT '01. Springer-Verlag, 2001: 453-474

[2] LaMacchia B, Lauter K, Mityagin. A Stronger security of authenticated key exchange[C]// Lecture Notes in Computer Science 4784. Berlin: Springer, 2007: 1-16

[3] Krawczyk H. HMQV: A High-Performance Secure Diffie-Hellman Protocol[C]// Advances in Cryptology CRYPTO'05, LNCS3621. Springer-Verlag, 2005: 546-566

[4] Cas J F, Cremers. Formally and practically relating the CK, CK-HMQV and eCK security models for authenticated key exchange [OL]. http://eprint.iacr.org/2009/253.pdf

[5] Cheng Qing-feng, Ma Chuang-gui, Wei Fu-shan. A modified eCK model with stronger security for tripartite authenticated key exchange[OL]. http://eprint.iacr.org/2010/042.pdf

[6] Zhao Jian-jie, Gu Da-wei. Provably secure two-party authenticated key exchange protocol in eCK model[J]. Chinese journal of computers, 2011, 34(1)

[7] Zhou Qing-lei, Yang Zeng-fu. TUP: A new eCK-secure AKE protocol under the CDH assumption[J]. International Journal of Communications, Network and System Sciences, 2012: 5(6): 332

[8] Pan Jin-xin, Wang Li-lin. TMQV: A strongly eCK-secure Diffie-Hellman protocol without Gap assumption[J]. Journal of international services and informatin security, 2012, 1(2/3): 107-124

[9] Fujioka A, Suzuki K. Designing Efficient Authenticated Key Exchange Resilient to Leakage of Ephemeral Secret Keys[J]. Lecture Notes in Computer Science, 2011, 6558: 121-141

[10] Ustaoglu B. Obtaining a secure and efficient key agreement Drotocol from(H) MQV and NAXOS[J]. Designs, Codes and Cryptography, 2008, 46(3): 329-342

[11] 贾小英，李宝，刘亚敏. 随机谕言模型[J]. 软件学报，2012，23(1) 141-151