# 一种基于 Diffie－Hellman 体制的 XML 安全传输方案

## A XML Security transmission Scheme Based on the Diffie－Hellman Protocol

李　甜　王泽兵　（浙江大学城市学院 310027）
冯　雁　（浙江大学计算机学院 310027）

**摘要**：可扩展标记语言 XML 因其诸多优点，成为互联网应用及电子商务的标准描述语言。随着 XML 技术的发展，其安全性问题越来越不容忽视。本文根据 XML 的特点，应用 Diffie—Hellman 密钥交换体制以及 XML 加密、XML 签名技术，提出了一种基于 Diffie－Hellman 和 SSL/TSL 协议，并结合 XML 加密和 XML 签名技术的 XML 安全技术方案，解决了传统加密方案存在的一些不足。

**关键词**：XML 加密 XML 签名 Diffie－Hellman 协议 SSL/TSL 协议

## 1　引言

XML 因其良好的数据存储格式、可扩展性、高度结构化和便于网络传输等优点，很快就被广泛应用到各个领域，成为互联网应用及电子商务的标准描述语言。因此 XML 在存储和交换时的安全变的非常重要，XML 的安全性问题已经成为了一个不容忽视的问题。针对 XML 的安全性问题，W3C 组织提出了三种机制来保证 XML 的安全性：XML 加密，XML 签名以及 XML 密钥管理（XKMS）。

本文先对 Diffie－Hellman 密钥交换体制以及 XML 加密、XML 签名技术进行分析，然后提出一种基于 Diffie－Hellman 体制的 XML 安全技术方案，从而保证了 XML 数据传输的高速性、保密性、开放性、整体性和确认性。

## 2　Diffie－Hellman 协议

Diffie－Hellman 协议是一种密钥交换体制，其安全性是由大素数条件下的离散对数的不可计算性保证的。该算法可用于通信双方（或多方）的密钥交换，即各方按照 Diffie－Hellman 协议所规定的通信规则互换算法生成数，最后产生共用的对称密钥。

首先，甲乙通信双方协商并确定两个 Diffie－Hellman 参数：一个大素数 P 和一个大自然数 a，a 为模 P 的原根。根据“原根”定义则 a mod P，a^2 mod P，…，a^(P－1) mod P 各不相同，就是小于 P 的 P－1 个自然数。因此 a 与模 P 互质。这样，任何 1 到 P－1 之间的整数 k 都有一个对应整数 q 使得 k＝a^q mod P，P 和 a 的值可以公布或在甲乙方之间交换。

P 和 a 的选择对系统安全性有较大影响，应选择较大的 P（512 位以上），可以采用“强素数”：P 和（P－1）/2，a 和（a－1）/2 都是素数。

Diffie－Hellman 协议保证了在 Internet 上交换共享密钥的保密性，比手工传送或者通过“握手”方式传送更加便利。并且应用 Diffie－Hellman 密钥交换可以在需要的时候才创建密钥，可及时更新共享密钥，因而更能保证数据的安全性。

## 3　XML 加密和 XML 签名

目前常用于网上加密认证的是 SSL/TLS 协议，它提供了通信双方之间端到端的安全会话，已成为 Internet 上安全通信的事实标准。但随着 Internet 信息交换需求的发展，SSL/TLS 渐渐暴露出种种不足。例如：无法保证传输文档的不可抵赖性；不能做到加密交换数据的一部分；无法实现多方（不止两方）之间的安全会话；不能实现多级的重复加密或签名。作为 SSL/TLS 安全协议的完善和补充，2002 年 4 月 W3C 组织公布了最新的 XML 加密与签名规范，从对称加密算法（包括流加密、块加密算法）、密钥传输与协商、消息摘要、文档签名等方面进行了规范格式说明。

相比与传统的安全技术，XML 加密和 XML 签名可

对文件中部分数据进行签名和加密，并且可对任何数据内容进行操作，包括整篇 XML 文档、XML 元素、XML 元素的内容以及非 XML 数据，并且 XML 安全技术能保证数据在传输中的安全性，像 SSL 这样传统的安全技术是不能保证数据在传输中的安全性的，只能在发送和接收时保证其安全性。

### 3.1 XML 加密

(1) 对单个元素进行加密。在加密 XML 文档中某个元素的过程中，需要引入 <EncryptedData> 元素，<CipherData> 元素和 <CipherValue> 元素。其中，<EncryptedData> 包含用于加密的 XML 名称空间。而 <CipherData> 和 <CipherValue> 的主要功能是存储加密后的数据。XML 加密被嵌入到用户的 XML 中，既包含了 XML 加密模式又包含来自原始文档中的原始元素。

以下是加密 XML 文档中一个元素的加密结果：

```
<? xml version = "1.0" ? >
< PaymentInfo xmlns = " http://example. org/paymentv2" >
    <Name > Jim </Name >
    < EncryptedData xmlns = " http://www. w3. org/2001/04/xmlenc#"
      Type = " http:// www. w3. org/2001/04/xmlenc#Element" >
      <CipherData > <CipherValue > A23B45C56 </CipherValue > </CipherData >
    </EncryptedData >
</PaymentInfo >
```

原文档中要加密的元素被 <EncryptedData> 元素取代。<EncryptedData> 的 Type 属性值是 http://www. w3. org/2001/04/xmlenc#Element。其中的"#Element"表示 <EncryptedData> 中加密的是一个元素。

(2) 对元素的内容进行加密。在某些情况下，只需要隐藏一些敏感内容，此时用 XML 加密某一个元素的值即可。用 <EncryptedData> 元素取代要加密的元素值，并在 <EncryptedData> 的 Type 属性中指出加密的是元素的内容 Type = " http:// www. w3. org/2001/04/xmlenc#Content"

另外，如果不希望别人能够看到信用卡用户的任何信息，可以对整个 XML 文档进行加密。只需把 <EncryptedData> 的 Type 属性值设置为" http://www. isi. edu/in - notes/iana/assignments/media - types/text/xml"

总之，XML 加密(XML Encryption)允许用户对加密粒度进行控制，可以加密交换数据的一部分；而且多个用户可以在同一文档中交换安全的和非安全的数据，每一方都可以保持与任何通信方的安全或非安全状态，可以进行多方或多级之间的安全会话。它提供了用于 SSL/TLS 未涵盖的安全性需求的机制，保证了数据的机密性和一对多交流的开放性。

### 3.2 XML 签名

XML 签名是特定的 XML 语法，用于表示对任意数据内容的数字签名。使用 XML 数字签名可以保证数据的完整性、发送者的真实性，同时防止发送者抵赖。在数字签名中，签名元素 <Signature> 和数据对象的相对位置有 3 种可能：

(1) 封装签名。数据对象放在客体元素(object)中，签名元素就是数据对象的祖先元素；

(2) 被封装签名。签名元素作为数据对象的子孙元素；

(3) 分离签名。签名元素与数据对象相分离。

XML 数字签名的核心元素是 Signature 元素，它包含了数字签名的具体信息，<Signature> 元素必须包含的 SignedInfo 元素是实际签名的信息。<CanonicalizationMethod> 标识了一种算法，这种算法被用来规范化 SignedInfo 元素然后该元素作为签名操作的一部分被摘要。<SignatureMethod>，是用于将已规范化的 SignedInfo 转换成 SignatureValue 的算法。这是摘要算法、密钥从属算法和可能的其它算法的组合。<Reference> 的这个可选 URI 属性标识要签名的数据对象。<Transforms> 是一种可选的处理步骤排序列表，在摘要资源内容之前，要使用这些步骤。这是解密所需遵循的轨迹。加密、签名、修改和可能进行的更多签名所发生的顺序有很多种可能性。<DigestMethod> 是在应用 Transforms(如果已经指定它)之后对数据应用以产生 DigestValue 的算法。DigestValue 的签名是将资源内容与签名者密钥绑定的机制。<KeyInfo> 表示用于验证签名的密钥，标识机制可以包括证书、密钥名称和密钥协议算法。

进行 XML 数字签名时，可先从钥匙库中提取得到

用户的私钥，然后使用私钥对给定的 XML 格式文件进行签名操作（选择摘要算法，规范化，选择签名算法），生成签名文件；如果需要，可由可靠的时间服务器给签名文件加上时间戳（规定文件的有效期）。

## 4 基于 Diffie－Helman 体制的 XML 安全传输方案

### 4.1 加密过程

为了保证 Internet 上信息的安全传输，如果单独使用目前最著名的 RSA 加密体系，则存在加密速度慢，且一次处理的数据量不能大于其密钥的位数等缺点。因此一般设计采用 RSA 算法传送少量的、关键的数据。


图 1　总流程图

而传统的对称加密体系虽然加密速度较快，但其保密性集中在密钥的保密性上，加密方和解密方共同保存相同的密钥副本，当任何一个密钥副本失密时，所有的数据都是可破译的。所以如何将保密密钥从产生的一方安全传送到另一方是一个难点。在一些"端到端"的信息传送模式中，例如 B2B 电子商务，靠手工传送或者通过"握手协议"来分发交换共享密钥就显得不够便利且不安全，而且也无法实现共享密钥的及时更新。

为解决网上交换公共密钥的安全问题，我们考虑 Diffie－Hellman 密钥交换体制。其保密性基于求解离散对数问题的复杂性，在具有很好保密性的同时也不会影响在算法上选择对称加密算法。但 Diffie－Hellman 密钥交换体制有一个很大的弱点，就是难以进行身份验证，也无法避免插入重放攻击。如果破译者插在通信双方之间接力传送，就可以轻易地截取所有的信息。

因此本文提出一种基于 Diffie－Hellman 密钥交换体制的 XML 安全技术方案，数据传输双方用 Diffie－Hellman 密钥交换体制实现共享密钥网上交换的保密性；并通过 SSL/TSL 安全协议传输双方的 DH 公钥，用对方提供的数字证书来进行身份验证；当身份验证通过，双方根据自己的私钥和接收到的对方公钥计算获得共享密钥 K 后，用 K 对要传输的数据进行加密和签名；最后通过网络传输对称加密后的数据。

总流程如图 1 所示。

下文是一个甲方通过网络向乙方传输一个简单的 XML 文档 M 的示例。如下所示明文 M 包含了信用卡信息和其他个人信息。

```
<? xml version = "1.0" ? >
< PaymentInfo xmlns = " http://
example. org/paymentv2" >
    < Name > Jim < /Name >
    < CreditCard Limit = " 5,000"
Currency = " USD" >
        < Number > 4019 2445 0277
5567 < /Number >
        < Issuer > Bank of the Inter-
net < /Issuer >
        < Expiration > 04/02 < /Expira-
tion >
    < /CreditCard >
< /PaymentInfo >
```

(1) 甲乙通信双方协商并确定两个 Diffie－Hellman 参数：一个大素数 P 和一个大自然数 a，a 为模 P 的原根；

(2) 甲乙双方都随机选择一个与 P 互素且小于 P 的大整数 X 做为自己的私有密钥；

(3) 根据公式：$Y = a^X \bmod P$ $(0 < Y < P)$，甲乙双方各自计算出 Y 作为自己的 DH 公钥；

(4) 通过 SSL/TLS 协议，甲乙双方把自己的公钥 Y 发送给对方。如果发送者数字证书验证不通过，则公钥 Y 的传送失败；如果身份验证通过，则继续下一步；

(5) 甲乙双方根据自己的私钥 X 和接收到的对方公钥 Y，求出双方使用的共享密钥 K$(0 < K < P)$为：

$K1 = (Y2)^{X1} \bmod P$

$K2 = (Y1)^{X2} \bmod P$

K = K1 = K2；

(6) 甲方用求出的共享密钥 K 对要传输的 XML 文档进行对称加密(可选择加密整篇文档、单个元素或元素内容，这里选择加密文档 M 中的 <CreditCard> 子元素 <Number> 的内容)，并对文档进行摘要和签名。

(7) 甲方把经过加密和签名的 XML 文档通过网络发送给乙方；

### 4.2 验证解密过程

乙方接收该文档后，先验证甲方的 XML 签名，验证通过后再用求出的共享密钥 K 对密文 C 进行解密，从而得到原始 XML 文档 M。

具体流程如图 2 所示：

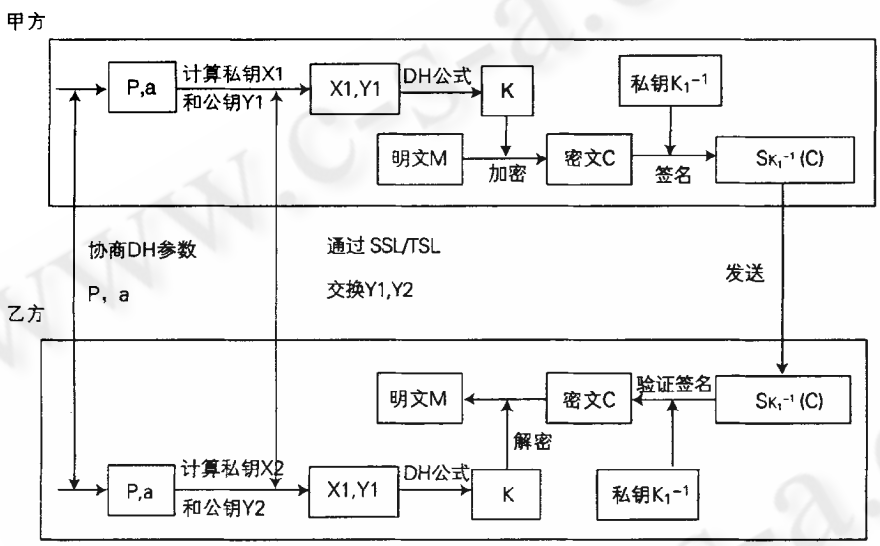


图 2　验证解密流程图

### 4.3 优缺点分析

本方案采用了 Diffie - Hellman 共享密钥交换体制，结合 SSL/TSL 协议和 XML 签名及加密。其核心是 XML 签名和 XML 加密这两项 XML 安全技术。这使得本方案能支持对任意数字内容的加密和签名；能确保经过加密的数据不管是在传输过程中还是在存储时，都不能被未经授权的人员访问；无论数据是正在传输的过程中还是在某个特定的节点停留的时候，都能保证其安全性；并以 XML 形式表现被加密和被签名的数据，保证了数据结构的完整性和可读性。

在有诸多优点的同时，方案在数字证书的发放、密钥的管理上还存在一些不足，如果进一步结合 XML - PKI 密钥管理技术，相信更能提高本方案实施过程中的便利性。

## 5 结束语

由于 XML 具有简单性、开放性、可扩展性、灵活性、自描述性等特性，它被广泛用于网络数据的交换和发布。随着 XML 技术的广泛应用和发展，安全性问题越来越成为研究热点。XML 加密和 XML 签名是 XML 安全技术的核心部分，可解决传统安全技术所存在的不足，能有效增强 WEB 资源的安全性。

XML 安全技术还处于发展阶段，还不是一个很完善的技术体系。把 XML 安全技术与传统的安全技术相结合、使其相互补充，是加强 XML 安全的便利性、可靠性和稳健性的一种手段。

### 参考文献


1 W3C 工作组. XML Encryption Syntax and Processing [EB/OL]. http://www.w3.org/TR/xmlenc-core/

2 W3C 工作组. XML - Signature Syntax and Processing [EB/OL]，http://www.w3.org/TR/xmldsig-core/.

3 Murdoch Mactaggart[EB/OL]，XML 加密和签名简介. http://www-900.ibm.com/developerWorks/cn/xml/sxmlsec.

4 曹珍富[M]，公钥密码学，黑龙江教育出版社，1993。

5 杨义先、林须端[M]，编码密码学，人民邮电出版社，1992。

6 (英) Mark Birbeck 等[M]，XML 高级编程(第二版)，北京机械工业出版社，2002。

7 Heather uilliamson[M]，XML 技术大全，北京机械工业出版社，2002。