XML联合签名

郑晓梅[1,3] 张 天[2,3]
(南京中医药大学信息技术学院 南京 210046)[1] (南京大学计算机系 南京 210093)[2]
(南京大学计算机软件新技术国家重点实验室 南京 210093)[3]

摘 要 首先分析了目前Web服务架构中XML多方通信业务链的典型应用,并建立了相应的研究模型。基于此模型,提出了联合签名加密技术,以解决传统签名技术在此类应用中存在的重复签名、信息关联不严格等问题。同时,分析了通过现有XML签名规范实现该技术的局限性,进而提出了新的XML联合签名实现方案。最后给出了XML联合签名的语法定义。

关键词 XML多方通信业务链,联合签名,XML签名,XML联合签名
中图法分类号 TP309.2 **文献标识码** A

XML United Signature

ZHENG Xiao-mei[1,3] ZHANG Tian[2,3]
(Institute of Information Technology, Nanjing University of Chinese Medicine, Nanjing 210046, China)[1]
(Department of Computer Science and Technology, Nanjing University, Nanjing 210093, China)[2]
(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China)[3]

Abstract This paper firstly analysed the typical application of the XML multi-party communication chain business in the current Web server architecture and built up the corresponding research model. Based on the model, this paper proposed a new encryption technology named untied signature, which can solve the problems of the reduplicate signature and not strict information association using the traditional signature technology. This paper also analysed the limitations of using current XML specification to fulfill the encryption technology, and then raised the implementation scheme of XML untied signature. Finally, this paper presented the syntax definition of XML united signature.

Keywords Chain business of XML multi-party communication, United signature, XML signature, XML united signature

1 引言

XML[1]已经成为一种用于Internet信息描述和信息交换的标准,并作为交换数据的载体广泛应用于Web服务中。

在目前Web服务架构应用中,经常出现很多XML多方通信业务链的应用,这些具体的业务链在事务处理过程中会出现一方需要向多方提供信息,将这些信息放在同一个XML文档提交给直接下游方。再根据业务处理的需要不断地在整个业务链中传递相关信息,且这些信息中可能部分或者全部都是敏感信息。

这些信息的敏感性一方面体现在具有一定的私密性,通信各方不希望彼此之间泄露信息,可以用数字信封对这些信息加密来达到目的;另一方面体现在通信过程中的确认性、完整性以及不可否认性问题,一般解决这个问题使用传统签名技术,具体的做法是使用信息发送方的私有密钥对这些需要发送给其他通信方的信息进行逐个签名,然后放在同一个XML文档提交给直接下游方,这种解决方法重复性极强,从而大大影响速度;另外不能把同一次业务中发送给各方的信息严格关联起来,下游方容易错误地接收到上游业务方提供的另一次业务的信息且通过验证,从而引起业务错位事故。

针对传统签名方法存在这样的重复签名、信息不严格关联问题,本文提出一种新的加密技术,即联合签名技术,用以对这些敏感信息做到一次性整体签名,各通信方独立部分验证自身信息,从而提高业务处理的效率和安全性。另外,对于实现XML文档的联合签名这一问题,现有的XML签名规范[2]并不能够很好地给与支持,本文进一步就如何实现对XML文档进行联合签名提出了XML联合签名的实现方案,并给出了方案的语法定义,包括语法结构、XML Schema[3]以及处理规则。

本文首先介绍了XML多方通信业务链,通过为XML多方通信业务链建立研究模型去分析XML多方通信业务中存在的安全问题以及解决方案所存在的问题,然后提出了联合

到稿日期:2009-09-18 返修日期:2009-12-07 本文受863国家高技术研究发展计划(No. 2007AA010302),国家自然科学基金(No. 60425204),江苏省自然科学基金(No. BK2007714)资助。
郑晓梅(1978—),女,讲师,主要研究方向为医学信息安全、中医特征信息建模与分析验证等,E-mail:zxm_luck@163.com;**张 天**(1978—),男,讲师,CCF会员,主要研究方向为模型驱动软件工程。

签名技术并分析了该技术的工作原理以及特点，之后讨论了XML联合签名实现方案提出的必要性，最后给出了XML联合签名的语法定义。

2 XML多方通信业务链

2.1 XML多方通信业务链的典型应用

申请办理健康保险流程（见图1）就是XML多方通信业务链一个典型应用实例，业务流程需要四方参与：申请人、保险公司、健康认证中心以及银行。在业务过程中，申请人需要向健康中心提交病历资料，需要向银行提供账号信息，以及需要向保险公司提供相关的保险申请信息。为了提高效率，申请人首先将所有信息通过一个XML文档发给保险公司，由保险公司在处理业务过程中将申请人的病历资料通过XML文档转发给健康中心进行认证；保险公司在得到健康中心的认证信息后，再向银行转发申请人的XML账号信息，由银行进行转账处理。

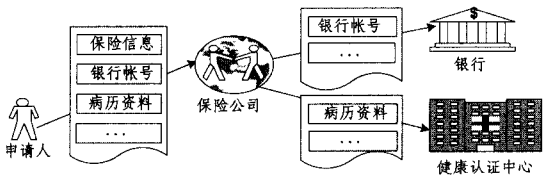

图1 申请办理健康保险流程

在整个业务流程中，不仅用户申请人的病历资料是敏感信息，银行账号信息以及保险信息也都是敏感信息，并且这两种信息都是用户在向保险公司提供资料时放在同一个XML文档中，由保险公司在处理业务中经过解析XML文档，再将相关信息用XML文档传递给下游业务方。

2.2 XML多方通信业务链的研究模型

在如今以Web服务为架构的业务流程中，类似于申请办理健康保险业务流程这样的XML多方通信业务链在日常生活中比比皆是，如办公自动化、住房贷款审批、病人住院申请等。为了方便问题的研究，本文首先根据这些典型应用的特点为XML多方通信业务链建立一个研究模型，如图2所示。

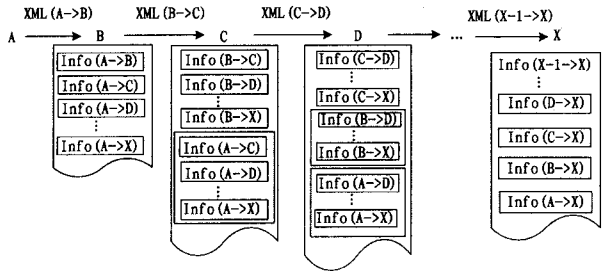

图2 XML多方通信业务链的研究模型

业务链由多个通信方A,B,C,D,…,X组成。要使得业务正常开展，下游业务方需要上游业务方通过XML文档传递一定的相关信息。如D业务方正常开展，在其直接上游业务方C方发送的XML文档中，除了有可能含有C方提供给D方的信息Info(C->D)，还可能含有C方转发的B方提供给D方的信息Info(B->D)，也可能含有C方转发的A方提供给D方的信息Info(A->D)。因此对于业务链模型，为了使得业务顺利，快速地开展，上游业务方往往会把发送给其所有下游业务方的信息放在同一个XML文档中一次性发送给直接下游业务方，再由直接下游方通过业务链层层传递下去。

2.3 XML多方通信业务链中数据传输安全问题

从模型可以清晰地看出，XML多方通信业务链上游业务方发送给所有下游业务方的信息会通过XML文档在业务链中不断传递，如A发送给B的XML文档中，除了含有A需要的B的信息Info(A->B)，还应该含有A需要提供给C的信息Info(A->C)，以及A需要提供给D的信息Info(A->D)等。而这些信息部分甚至全部都是敏感信息（为了达到解决问题的严格性和全面性，将这些信息全部假定为敏感信息），那么这些敏感信息组成了一个敏感信息流，如A方发送给所有下游业务方的敏感信息组成的信息流——(Info(A-B),Info(A-C),Info(A-D),…,Info(A-X))，如图3所示。这样一个业务链中多方通信时的敏感信息数据的安全性需求主要体现为如下两个方面：

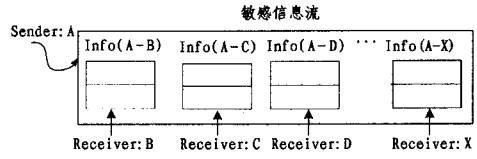

图3 A方发出的敏感信息流

(1)若各通信方之间不能互看敏感信息，又由于这些敏感信息可能会经过上游业务方的转发，因此要保证这些敏感信息在多方通信过程中的机密性；

(2)要保证这些敏感信息在多方通信过程的确认性、完整性和不可否认性。

要顺利开展此类业务链，就必须保证这些敏感信息的安全性，如何有效地保证这些敏感信息的安全性的课题就非常值得研究和探索。这就要求我们必须提出一个加密方案，为这些信息的传递建立一个安全的通信信道，并且此加密方案必须具有可行性好、保密性强、加密效率高的特点。对于第一个安全需求，可以采用数字信封技术[4,5]顺利地解决。数字信封技术结合了对称密钥加密技术和公开密钥加密技术的优点，可克服对称密钥加密中共享密钥分发困难和公开密钥加密中加密时间长的问题，使用两个层次的加密来获得公开密钥技术的灵活性和对称密钥技术的高效性，可保证信息的安全性。

对于第二个安全需求，传统的加密方法是对这些敏感信息逐个用发送方的私钥签名，然后将这些信息的摘要分发给接收方，由接收方用发送方的公钥进行验证。这种传统方法存在两个很严重的问题：

(1)重复签名问题。无论发送方是用RSA加密还是DSA加密，它们的签名速度都是很慢的。另外，发送方要对发送给所有下游业务方的敏感信息逐个进行数字签名，这些过程本身是重复而又冗余的。

(2)信息关联不严格问题。不能将同一次业务处理中的所有敏感信息严格关联，容易引起业务处理错位事故。因为信息或者信息密文本身以及信息签名摘要这一对数据都是经过业务链传递给接收方的，如果错发了另外一次业务处理过程相应的一对数据，那么只要信息没有被篡改，接收方就能通过信息验证，但是却不能检验出信息不是当次业务的处理信息。当然，解决这个问题也可以额外用时间戳等技术，但是这又要求发送方在逐个签名的基础上再用额外的技术，对于处

理速度而言是不可取的。

3 联合签名技术

3.1 联合签名技术的由来

基于以上描述，用传统的签名技术来保证 XML 多方通信业务链敏感信息的确认性、完整性以及不可否认性，会存在重复签名、信息关联不严格等问题。针对这一问题，本文提出了一种新的加密技术——联合签名技术。

联合签名技术是基于 SET 协议[6,7]的双重签名技术提出的。双重签名技术(Dual signature)是 SET 电子支付协议中的一项重要的加密技术，用于用户在使用信用卡进行电子商务交易时保证客户的信用卡信息和订购信息的隐私安全。本文通过反复研究双重签名技术，将双重签名技术的加密原理加以扩展、改进，从而提出了联合签名技术。将联合签名技术应用到一个 XML 多方通信业务链中，用来保证多方通信时敏感信息流的身份验证和信息完整性、交易防抵赖的保护，且可解决重复签名、信息关联不严格的问题。

3.2 联合签名技术的工作原理

为了叙述的完整性，本文首先为敏感信息流的通信建立一个安全信道。该信道采用数字信封技术来保证信息的机密性，采用联合签名技术来保证这些信息的确认性、完整性和不可否认性，通过介绍这个安全信道的工作原理来说明联合签名的工作原理；另外，为了叙述方便，以如何保证上述 A 方向其他下游业务方传递的敏感信息流(Info(A－B)，Info(A－C)，Info(A－D)，…，Info(A－X))的安全性为例来介绍这个安全信道。

(1) 加密过程(见图 4)

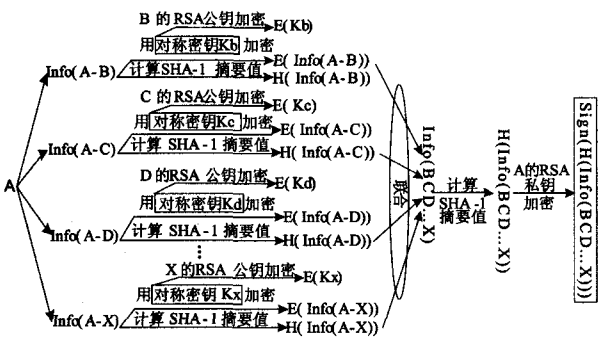

图 4 安全信道加密过程

1) A 端对(Info(A－B)，Info(A－C)，Info(A－D)，…，Info(A－X))分别用数字信封技术加密；

A 产生对称密钥 Kb，用 Kb 加密 Info(A－B)，产生密文 E(Info(A－B))；使用 B 的 RSA 公钥加密对称密钥 Kb 产生 E(Kb)；

同理产生 E(Info(A－C))，E(Kc)；E(Info(A－D))，E(Kd)；…；E(Info(A－X))，E(Kx)。

2) A 端对这些所要发送的敏感信息进行联合签名；

A 使用 SHA-1 摘要算法分别生成这些敏感信息的摘要值，记为 H(Info(A－B))；H(Info(A－C))；H(Info(A－D))；…；H(Info(A－X))；

A 联合所有这些敏感信息的摘要值 Info(BCD…X)，对其进行 SHA-1 摘要计算，生成摘要值，记为 H(Info(BCD…X))，并且 A 使用自己的 RSA 私钥对 H(Info(BCD…X))进行加密，生成 Info(BCD…X)的签名值，记为 Sign[H(Info(BCD…X))]，即 Sign[H(Info(BCD…X))]是对 Info(A－B)，Info(A－C)，Info(A－D)，…，Info(A－X)这些敏感信息的联合签名值。

(2) 信息发送

各业务方通过业务链的传递最终得到 XML 文档中一定包含以下几部分信息(以业务方 D 方为例)：

- 密文 E(Info(A－D))；
- 用 D 方的公钥加密对称密钥的结果 E(Kd)；
- 其他各方信息的摘要：H(Info(A－B))，H(Info(A－D))，…，H(Info(A－X))；
- 联合签名值：Sign[H(Info(BCD…X))]。

(3) 验证及解密过程(见图 5)

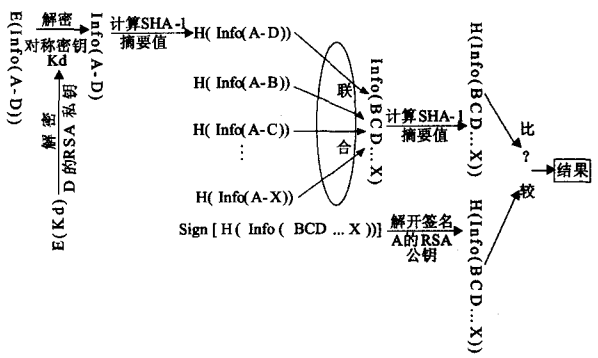

图 5 安全信道的解密及验证过程

以 D 方为例说明解密及验证工作原理。

1)D 方用自己的 RSA 私钥对 E(Kd)解密，得到对称密钥 Kd；

2)D 方用 Kd 对密文 E(Info(A－D))解密，得到 Info(A－D)；

3)D 方对 Info(A－D)进行 SHA-1 摘要计算，得到 Info(A－D)的摘要值 H(Info(A－D))；

4)D 方将计算的 H(Info(A－D))与接收到的其它各方敏感信息的摘要值 H(Info(A－B))，H(Info(A－C))，…，H(Info(A－X))相联合，得到联合值 Info(BCD…X)；

5)D 方对联合值 Info(BCD…X)进行 SHA-1 的摘要计算，得到摘要值 H(Info(BCD…X))；

6)D 方使用 A 的公钥对 Sign[H(Info(BCD…X))]进行解密，得到 H(Info(BCD…X))；

7)D 方将这两个 H(Info(BCD…X))进行比较，若相同，则表明 Info(A－D)信息是由 A 提供的，而且没有被篡改；另外，其他各方都看不到 Info(A－D)，虽然 Info(A－D)可能经过其他方转发。

4 联合签名技术的特点

联合签名技术是本文提出的一种新的签名技术，在应用中可以结合其他加密技术来建立具体的通信安全信道。如为了保证申请人向保险公司提供的敏感信息流(包括保险信息、用户帐号信息、病历资料)的安全，可以在这些信息发送前，建立一个基于联合签名的安全信道来保证这些敏感信息的安全。联合签名之所以没有传统签名技术所存在的重复签名、信息不严格关联的问题，是因为联合签名本身具有可行性好、保密性强、加密效率高的特点。

(1)从技术角度讲，联合签名技术具有的技术优势可以概

括为整体签名、部分验证；

1)发送方对某次业务处理提供给其他业务方的所有敏感信息只做了一次联接签名，不仅大大优化了签名速度，还能够将各部分敏感信息连接在一起，表明它们是同时被签发的，确保各业务方通过对联合签名值的验证就能够判断接收到的信息是否是这次业务的信息，排除了多次转发过程中业务错位事故发生的可能性。

2)接收方只需要知道签发联合签名者是谁，不必了解其他各业务方的身份，便可对自己的那部分信息进行正确验证。另外，虽然发送方在联合签名时对所有信息进行了联接签名，而接收方在验证时却无法看到发送方提供给其他各接收方的敏感信息(因为这些敏感信息一般都是以密文出现)，更无法对这些敏感信息加以验证。但是，由于联合签名特殊的加密机制，业务处理过程中某个业务方验证联合签名如果失败，也不会导致整个业务链的失败，因为这个业务方都可以向信息的提供方重新申请这部分敏感信息并进行业务处理，但不会影响业务链的其他业务环节的正常处理流程，这大大提高了业务处理的效率。

(2)从应用方面讲，在 Web 服务架构下由于多方通信业务链是采用 XML 文档作为数据传输的载体，使得联合签名技术的特点得到很好的体现和发挥。一个 XML 文档可以携带联合签名所产生的所有信息，从而大大减少了交互的复杂度，提高了效率。另外，可以摒弃业务方平台之间的差异，满足了互联网和分布式异构环境下的应用。任何中间业务方可以根据业务的需要对接收到的 XML 文档的内容进行增加或删除，使得整个业务处理很灵活。

5 XML 联合签名实现方案的提出

第 4 节中分析了联合签名技术在 XML 多方通信业务链应用中的重要意义。那么，如何实现在 XML 文档中进行联合签名？要实现这一目标，最为核心的问题就是实现对同一个 XML 文档中的多个信息的整体签名、部分验证。

现有的 XML 签名规范能不能很好地支持对 XML 文档进行联合签名？根据 2008 年 6 月 XML 签名语法与处理(第二版)，如果抛开 Manifest 元素定义这一非强制性部分而言，只能达到对 XML 文档中的信息进行整体签名、整体验证及部分签名、部分验证的目的。

本文要特别指出的是 XML 签名规范非强制性元素——Manifest 元素，它的内容是原本放置在 SignedInfo 元素中的多个 Reference 元素，如图 6 所示。

```
[ ]…
[m01] 〈Reference URI="#MyFirstManifest"〉
[m02]    Type="http://www.w3.org/2000/09/xmldsig#Manifest"〉
[m03]  〈DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/〉
[m04]  〈DigestValue〉345x3rvEPO0vKtMup4NbeVu8nk=〈/DigestValue〉
[m05] 〈/Reference〉
[ ]…
[m06] 〈Object〉
[m07]  〈Manifest Id="MyFirstManifest"〉
[m08]    〈Reference〉
[m09]      …
[m10]    〈/Reference〉
[m11]    〈Reference〉
[m12]      …
[m13]    〈/Reference〉
[m14]  〈/Manifest〉
[m15] 〈/Object〉
```

图 6 XML 签名规范中的 Manifest 元素

Manifest 元素的定义是为了满足 XML 签名的两个可能的额外要求而提出的。这两个额外要求以及它们的解决方案如下：

第一个，应用程序想要用不同的密钥分别签发一些数据对象，则把所有表示数据对象的 Reference 元素放在同一个 Manifest 元素中，这样就可以用不同的密钥签发 Manifest 元素，以提高效率。

第二个，XML 规范强制性部分规定：放置在 SignedInfo 元素中的所有的 Reference 元素都必须验证，如果其中一个验证失败，整个签名验证就会失败。如果不希望对每个 Reference 元素都验证，Manifest 元素对这个问题的解决方案是：将这些 Reference 元素分离出来，作为 Manifest 元素的子元素，然后可以由应用程序决定是否验证这些 Reference 元素以及验证失败后的处理。

第二个额外要求只是非常含蓄地暗示了在 XML 签名的实际应用中可能会存在整体签名、部分验证的要求，但是 XML 签名规范并没有明确地将这类要求总结提炼出来，也没有讨论它的应用范围。另外 Manifest 元素所给出的解决方案似乎可以实现对 XML 进行联合签名，但是这太费力、太牵强。原因如下：1)Reference 元素中没有属性或子元素来强制表示其应由哪个业务方验证，而是将决定验证哪个 Reference 元素的任务全部抛给应用程序。应用程序往往要分别读取出各个 Reference 元素所表示的数据对象后才能决定哪些 Reference的验证结果是本业务方所关心的。这使得应用程序负荷太重。而且，如果这些数据对象需要解密，应用程序可能会无能为力。业务方在处理 XML 联合签名时，应该能够容易地决定需要对哪些数据对象进行摘要计算。2)联合签名验证时，首先计算发送方提供给自己那部分信息(如 PI)的摘要，再将此计算的摘要值(记为 A)和其他所有的摘要值相连接，然后对这个连接值进行验证，而忽略 A 值是否与接收消息所提供的那个相应的摘要值相符合。这又和 XML 签名规范所给出的 Reference 元素的验证规则相悖。

通过以上分析，一方面由于对 XML 进行联合签名有很好的应用前景，另一方面由于 W3C 的 XML 签名规范没有明确地提出对 XML 进行联合签名的问题，并且给出的解决方案比较牵强，因此为了实现对 XML 文档中的多个信息进行联合签名，必须提出一个 XML 联合签名的实现方案。

6 XML 联合签名的语法定义

本文以 XML 签名规范为基础，通过扩展该规范所定义的语法和处理规则定义了 XML 联合签名的语法。

6.1 XML 联合签名的结构设计(见图 7)

```
〈UnitedSignature Id?〉
 〈SubDigests〉
  (〈SubDigest id?〉
   〈DigestInfo〉
    〈DigestReference (URI=)?〉
     (〈Tranforms〉) *
    〈/DigestReference〉
    〈DigestMethod/〉
   〈/DigestInfo〉
   〈DigestValue〉
  〈/SubDigest〉)+
 〈/SubDigests〉
 〈ds:Signature〉
 〈UnitedSignatureObject〉 *
〈/UnitedSignature〉
```

图 7　联合签名的语法结构

UnitedSignature 元素是 XML 联合签名的核心元素，包括 SubDigests，Signature 和 UnitedSignatureObject 子元素。SubDigests 元素包括多个 SubDigest 子元素，SubDigest 代表参加联合签名中的一个信息的摘要信息；Signature 元素包含联接摘要信息、联合签名信息和值、引用 XML 签名规范的定义；UnitedSignatureObject 元素放置其他信息，可能包括数据对象、时间戳等，其中数据对象可能是 EncryptedData 或者 EncryptedKey 所表示的密文数据。

6.2　XML 联合签名的 XML Schema 设计

XML 联合签名基于 XML 签名规范，在 XML 联合签名所设计的 XML Schema 文档 UnitedSignature. xsd 中引入了 W3C XML 签名的命名空间。XML 联合签名的 XML Schema 如图 8 所示。

```
〈? xml version= '1. 0' encoding= 'UTF-8' ? 〉
〈xsd:schema xmlns:xsd= ' http://www. w3. org/2001/
            XMLSchema'
            xmlns= '…/XMLSecurity'
            targetNamespace= '…/XMLSecurity '
            xmlns:ds= 'http://www. w3. org/2000/09/xmldsig#'
            elementFormDefault= 'qualified'
            attributeFormDefault= 'unqualified' 〉
 〈xsd:import namespace= 'http://www. w3. org/2000/09/xmldsig
             #' schemaLocation = ' http://www. w3. org/TR/
             2002/REC-xmldsig-core-20020212/xmldsig-core-sche-
             ma. xsd '/〉
 〈xsd:element name= 'UnitedSignature' type= 'UnitedSignature-
Type' /〉
 〈xsd:complexType name= 'UnitedSignatureType' 〉
  〈xsd:sequence〉
   〈xsd:element ref= 'SubDigests'/〉
   〈xsd:element ref= 'ds:Signature' /〉
   〈xsd:element name= 'UnitedSignatureObject' type= 'ds:Ob-
              jectType' maxOccurs= 'unbounded' /〉
  〈/xsd:sequence〉
  〈xsd:attribute name= ' Id ' type= ' ID ' use= ' optional ' /〉
   〈 xsd: anyAttribute namespace = ' http://www. w3. org/
XML/1998/namespace ' /〉
  〈/xsd:complexType〉
 〈xsd:element name= ' SubDigests ' type= ' SubDigestType ' /〉
 〈xsd:complexType name= ' SubDigestType ' 〉
  〈xsd:sequence〉
   〈xsd:element name= ' SubDigest ' maxOccurs= ' unbounded ' /〉
    〈xsd:complexType 〉
     〈xsd:sequence〉
      〈xsd:element ref= ' DigestInfo ' / 〉
      〈xsd:element name= ' DigestValue ' type= ' ds:Di-
gestValueType ' /〉
     〈/xsd:sequence〉
     〈xsd:attribute name= ' Id ' type= ' ID ' use= ' optional ' /〉
     〈xsd:attribute name= ' To ' type= ' String ' use= ' re-
quired ' /〉
      〈/xsd:complexType〉
   〈/xsd:sequence〉
  〈/xsd:complexType〉
 〈xsd:element name= ' DigestInfo ' type= ' DigestInfoType ' /〉
 〈xsd:complexType name= ' DigestInfoType ' 〉
   〈xsd:sequence〉
  〈xsd:element name= ' CanonicalizationMethod ' type= ' ds:Ca-
nonicalizationMethodType ' / 〉
  〈xsd:element name= ' DigestMethod ' type= ' ds:DigestMethod-
Type ' /〉
  〈xsd:element name= ' DigestReference ' type= ' DigestReferen-
ceType ' /〉
     〈xsd:complexTy pe 〉
          〈xsd:sequence〉
       〈xsd:element ref='ds:Transforms' minOccurs='0'/〉
          〈/xsd:sequence〉
      〈xsd:attibute name='Id'type='ID'use='optional'/〉
      〈xsd:attibute name= ' URI ' type= ' anyURI ' use=
' required ' /〉
    〈/xsd:complexType〉
    〈/xsd:sequence〉
 〈/xsd:complexType〉
〈/xsd:schema〉
```

图 8　XML 联合签名的 XML Schema

UnitedSignature 元素：是 XML 联合签名的根元素，有 3 个子元素——SubDigests 元素、Signature 元素和 UnitedSignatureObject 元素。

SubDigests 元素：SubDigests 元素表示发送给所有业务方的摘要信息，至少包含一个 SubDigest 元素。SubDigests 元素必须出现而且只能出现一次。

SubDigest 元素：表示发送给某个业务方的信息的摘要值及相关信息，包括两个子元素——DigestInfo 元素和 DigestValue 元素。DigestInfo 表示生成摘要的相关信息，DigestValue 表示摘要值，其中 DigestValue 的类型是 ds：DigestValueType。SubDigest 元素有两个属性——Id 属性和 To 属性，To 属性的值表示该 SubDigest 元素应由“谁”来处理。

DigestInfo 元素：表示生成摘要的相关信息，包括 3 个子元素——CanonicalizationMethod 元素、DigestMethod 元素和 DigestReference 元素。其中 CanonicalizationMethod 元素表示标准化计算摘要数据对象的算法信息，其类型为 ds：CanonicalizationMethodType；DigestMethod 元素表示摘要算法

的信息，其类型为 ds:DigestMethodType；DigestReference 元素表示被计算摘要的数据对象的信息。

DigestReference 元素：表示被计算摘要的对象的信息，URI 属性和 ds:Transforms 元素用来描述如何得到被计算摘要的内容。可选的 ID 属性可以允许从其他地方指向该 DigestReference 元素。

Signature 元素：其类型是 ds:SignatureType，用来表示联合签名的签名信息和值。其中 Reference 元素的子元素 Transforms 用来表示如何得到那些要被连接的所有的摘要值，DigestMethod 和 DigestValue 分别表示连接值的摘要算法和摘要值；SignatureMethod 元素表示联合签名的签名算法；SignatureValue 元素表示联合签名值。

UnitedSignatureObject 元素：其类型是 ds:Object，用来放置其他信息，可能包括数据对象、时间戳等。数据对象可能是由 EncryptedData 或者 EncryptedKey 表示的密文数据。

6.3 XML 联合签名的处理规则

(1)产生 XML 联合签名

第一步　构建 SubDigest 元素(这个过程是个循环的过程)。

选择摘要计算数据对象，规范化该数据对象，选择摘要算法，计算摘要值，构建 DigestValue 元素；

构建 DigestInfo 元素；

构建指定规范化数据对象算法的 ds:CanonicalizationMethod 元素；

构建表示摘要算法的 ds:DigestMethod 元素；

构建表示如何得到摘要计算数据对象的 DigestReference 元素(包括指定表示数据对象的引用属性 URI 和表示转换列表的子元素 ds:Transforms)；

标明此元素应交给哪个业务方处理，用业务方的代号来表示 To 属性的值。

第二步　将各个 SubDigest 元素放在一起，构建 SubDigests 元素。

第三步　构建 ds:Signature 元素(其中用 ds:Reference 元素来表示需要连接的所有的子摘要和联接摘要值，用 ds:SignatureValue 元素来表示联合签名值)。

第四步　构建 UnitedSignatureObject 元素(其中如果要表示数据密文，则遵从 XML 加密规则来构建 EncryptedData 元素并替换数据对象明文)。

第五步　构建 UnitedSignature 元素。

(2)验证 XML 联合签名

第一步　替换摘要值。

1)从 SubDigests 元素中通过 SubDigest 元素的 To 属性值找到本业务方应处理的那些 SubDigest 元素；

2)通过 SubDigest 元素的 DigestInfo 子元素的 DigestReference 元素得到被计算摘要的数据对象。其间，要通过 DigestReference 的 URI 属性表示的数据对象引用和子元素 ds:Transforms 表示的转换列表得到目标数据对象(若有解密转换，需要对 EncryptedData 元素解密)；

3)根据 Digest 元素给出的规范化算法规范化上面所得的数据对象，并根据 Digest 元素给出的摘要算法计算规范化后的数据对象的摘要值；

4)用此摘要值替换 DigestValue 元素的内容。

第二步　验证 ds:Signature 元素。

处理规则中要涉及到 XML 加密/解密和 XML 签名/验证，这些过程的处理规则符合 W3C XML 加密规范和 XML 签名规范，可以参考这两个规范。

7 相关工作

本文工作的特点是提出了一种新的签名技术即联合签名技术，它在用于保证 XML 多方通信业务链敏感信息流的数据的完整性时明显具有安全性高、效率高、应用前景好的优势。另外，本文就如何实现 XML 文档的联合签名提出了 XML 联合签名的实现方案，作为对现有的 XML 签名规范的补充。本文对 Web 服务架构中的具体应用的特定安全问题的处理更加完善、可行。以往这方面的研究工作主要有两个方向，一是研究如何实现 XML 安全技术；二是对于实际应用中需要的一些签名技术提出具体的实现方案，以补充现有的 XML 签名规范。

文献[8]指出，保证电子病历法律效力需要解决的安全问题是实现对电子病历的多重签名，然后基于目前 XML 签名规范，给出了电子病历文档签名与验证的实现 API 接口。但是文献[8]中的多重签名不是一种新的加密技术，现有的 XML 签名规范也是可以对 XML 文档实现多重签名的。他们工作的侧重点在于设计实现 XML 多重签名的 API 接口。相似地，文献[9,10]都是阐述 XML 安全技术的具体实现以及实现中存在的问题。

文献[11]指出了在 Web 服务架构中存在的一些线性商务链的应用，在线性商务链中存在商业文档，这些 XML 文档中的集成数据由不同的实体提供，这些数据可以用 XML 签名规范去实现某些部分数据的完整性。但是在实际的应用场景中，需要对 XML 文档进行可净化签名，也就是允许线性商务链中的被授权方修改签名文档的指定部分。现有的 XML 规范不支持可净化签名，文献[11]讨论了可净化签名在 Web 服务应用中的重要性和必要性，进而给出了实现方案，作为对 XML 签名规范的补充。文献[11]的工作和本文工作的目的比较相似，虽然可净化签名不是该文献提出的签名技术，但是给本文的研究工作提供了思路。

结束语　本文通过描述 Web 服务架构下一些常见的、典型的 XML 多方通信业务链应用实例，总结了这些典型应用实例的特点并为这类应用建立了研究模型，提出了 XML 多方通信业务链中敏感信息流在传输过程中的安全需求，分析了保证这些安全需求的解决方案，发现用传统的签名方法来保证这些敏感信息流传输时的确认性、完整性和不可否认性存在着重复签名、信息不严格关联的严重问题。

本文通过研究 SET 电子支付中的一项重要加密技术——双重签名加密技术，沿用双重签名技术的优势对其进行扩展、改进，从而提出了一种新的加密技术——联合签名技术。联合签名技术具有对同一个 XML 文档中的多个信息进行整体签名、部分验证的技术特点，能够克服传统签名存在的重复签名、信息不严格关联的问题。在实际应用中可以结合数字信封技术建立安全信道，以保证 Web 服务架构下 XML 多方通信业务链敏感信息流的安全性。本文在总结联合签名的技术特点、良好应用前景的基础上，讨论了现有的 XML 签

(下转第 247 页)

[11] Sarawagi S, Bhamidipaty A. Interactive deduplication using active learning[C]// Proc. KDD-02. 2002:269-278

[12] Bilenko M, Mooney R. On evaluation and training-set construction for duplicate detection[C]// Proc. KDD-03 Workshop on Data Cleaning, Record Linkage, and Object Consolidation. 2003: 7-12

[13] Cohen W, Ravikumar P, Fienberg S. A comparison of string metrics for matching names and records[C]// Proc. KDD-03 Workshop on Data Cleaning, Record Linkage, and Object Consolidation. 2003:13-18

[14] Tejada S, Knoblock C, Minton S. Learning domain-independent string transformation weights for high accuracy object identification[C]// Proc. KDD-02. 2002:350-359

[15] Bilenko M, Mooney R. Adaptive duplicate detection using learnable string similarity measures[C]// Proc. KDD-03. 2003:39-48

[16] Cohen W, Kautz H, McAllester D. Hardening soft information sources[C]// Proc. KDD-00. 2000:255-259

[17] Noren G, Orre R, Bate A. A hit-miss model for duplicate detection in the WHO Drug safety Database[C]// Proc. KDD-05. Chicago, IL, 2005:459-468

[18] Davis J, Dutra I, Page D, et al. Establishing identity equivalence in multi-relational domains[C]// Proc. ICIA-05. 2005

[19] Li X, Morie P, Roth D. Semantic integration in text: from ambiguous names to identifiable entities[J]. AI Magazine, 2005, 26 (1):45-58

[20] Huang T, Russell S. Object identification : a Bayesian analysis with application to traffic surveillance[J]. Artificial Intelligence, 1998, 103(1/2):77-93

[21] Singla P, Domingos P. Object identification with attribute-mediated dependences[C]// Proc. PKDD-05. Porto, Portugal, 2005: 297-308

[22] Dong X, Halevy A, Madhavan J. Reference reconciliation in complex information spaces[C]// Proc. SIGMOD-05. 2005:85-96

[23] Culotta A, McCallum A. Joint deduplication of multiple record types in relational data[C]// Proc. CIKM-05. 2005:257-258

[24] Singla P, Domingos P. Entity resolution with Markov logic[C]// Proc. of the 6th IEEE International Conference on Data Mining (ICDM2006). Hong Kong, China, December 2006:572-582

[25] Dzeroski S, Blockeel H, et al. Multi-Relational Data Mining 2004: Workshop Report[C]// Proc. of the KDD-04 Workshop on Multi-Relational Data Mining. Chicago, IL, 2004:140-141

[26] Jordan M I. Graphical models [J]. Statistical Science (Special Issue on Bayesian Statistics), 2004, 19(1):140-155

[27] Baader F, Calvanese D, McGuinness D L, et al. The Description Logic Handbook: Theory, Implementation, Applications [M]. Cambridge, UK: Cambridge University Press, 2003

[28] Richardson M, Domingos P. Markov logic networks[J]. Machine Learning, 2006, 62(1/2):107-136

[29] Gu D, Du J, Pardalos P. The Satisfiability Problem: Theory and Applications[M]. American Mathematical Society, New York, NY, 1997:573-586

[30] Gilks W R, Richardson S, Spiegelhalter D J. Markov Chain Monte Carlo in Practice [M]. London, UK: Chapman and Hall, 1996

[31] Richardson M, Domingos P. Markov logic networks[J]. Machine Learning, 62(1/2):107-136, 2006

[32] Singla P, Domingos P. Discriminative training of Markov logic networks[C]// Proc. AAAI-05. Pittsburgh, PA, 2005:868-873

[33] Kok S, Domingos P. Learning the structure of Markov logic networks[C]// Proc. of the 22nd International Conference on Machine Learning (ICML2005). Bonn, Germany, August 2005: 441-448

[34] Richardson M, Domingos P. Markov logic: a unifying framework for statistical relational learning[C]// Proc. of the ICML-2004 Workshop on Statistical Relational Learning and its Connections to Other Fields. Banff, Alberta, Canada, July 2004:49-54

[35] 刘大有，于鹏，高滢，等. 统计关系学习研究进展[J]. 计算机研究与发展，2008，45(12)

[36] 孙舒杨，刘大有，孙成敏，等. 统计关系学习模型 Markov 逻辑网综述[J]. 计算机应用研究，2007，24(2)

(上接第 213 页)

名规范无法实现对 XML 文档进行联合签名，从而提出了 XML 联合签名的实现方案；并以现有的 XML 加密规范以及 XML 签名规范为基础，为 XML 联合签名进行了语法定义，包括语法结构、XML Schema 以及处理规则。

在下一步工作中，将基于 Eclipse 环境来实现 XML 联合签名平台，用于支持 XML 文档中多个信息联合签名的实现。

参 考 文 献

[1] W3C. Extensible Markup Language(XML) 1.0(Fifth Edition) [EB/OL]. http://www.w3.org/TR/2008/REC-xml-20081126/, 2008

[2] W3C. XML Signature Syntax and Processing(Second Edition) [EB/OL]. http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/, 2008

[3] Walmsley P. Definitive XML Schema[M]. Prentice Hall PTR, 2001

[4] Trappe W, Washington L C. Introduction to Cryptography with Coding Theory[M]. 2nd edition. Prentice Hall, 2005

[5] Mason S. Electronic Signatures in Law[M]. second edition. Tottel, 2007

[6] Visa, MasterCard Inc. Secure Electronic Transaction Specification[EB/OL]. Version 1.0. http://www.visa.com/set, May 1997

[7] Kim H K, Kim T H. Design on Mobile Secure Electronic Transaction Protocol with Component Based Development[C]// Lecture Notes in Computer Science, ICCSA. 2004:461-470

[8] 陈乐君，石锐，李初民. 基于 XML 多重签名的电子病历安全机制[J]. 计算机科学，2007，34(12):136-138，170

[9] Knap T, Mlynková I. Towards More Secure Web Services: Pitfalls of Various Approaches to XML Signature Verification Process[C]// Icws. 2009:534-550

[10] Wang Wei, Li Jun. An XML Firewall on Embedded Network Processor[C]// icns. 2008:1-6

[11] Tan K W, Deng R H. Applying Sanitizable Signature to Web-Service-Enabled Business Processes: Going Beyond Integrity Protection[C]// Icws. 2009:67-74