# 跨组织安全物品追溯

韩伟力[1], 王 蔚[1], 张 胤[1], 袁 琅[1], 沈 烁[2], 王晓阳[1]

[1]复旦大学 软件学院 上海市数据科学重点实验室(复旦大学) 上海 中国 201203
[2]中国科学院计算网络信息中心 北京 中国 100190

**摘要** 由于供应链的应用场景往往需要多个公司的协同，物品追溯服务也就涉及跨组织的场景，因此有必要研究跨组织安全物品追溯的理论和方法。本文提出一个跨组织物品追溯的形式化模型和跨组织物品追溯服务的三个安全属性：可追溯性、可信性和隐私保护；设计一个跨组织安全物品追溯框架，及其中的三个基本协议：发货协议、验证协议和收货协议；本文最后介绍一个满足上述三种安全属性的跨组织安全物品追溯原型系统，并对其进行评估。

**关键词** 物品追溯；供应链；跨组织；数据安全
**中图法分类号** TP309.2

# Cross-Organizational Secure Object Tracking

HAN Weili[1], WANG Wei[1], ZHANG Yin[1], YUAN Lang[1], SHEN Sean[2], WANG X. Sean[1]

[1] Shanghai Key Laboratory of Data Science, Fudan University, Software School, Shanghai 201203, China
[2] Computer Network Information Center, CAS, Beijing 100190, China

**Abstract** To solve the data security problem for object tracking in a cross-organizational supply chain, a formal model with three security properties, i.e., accountability, trustworthiness, and privacy protection, is introduced. The model may be implemented with three protocols introduced in the paper, namely goods issuing, validation, and goods receipt protocols. The above formal model and the associated protocols are evaluated through a prototype implementation described in the paper, along with an analysis of its performance.

**Key words** tracking; supply chains; cross-organizational; data security

## 1 前言

物联网 (Internet of Things, IoT) 技术自提出后便得到了高速发展。其中，无线射频技术 (Radio Frequency Identification, RFID)[1]、传感器技术等已被广泛应用在医药服务[2]、食品供应[3]、安全采矿等各个领域中。在物联网的各种应用场景中，针对物品的追溯服务成了物联网技术飞速发展中一个杀手级应用，并已广泛地部署在物联网相关的组织机构中[4,5,26]。在物联网领域常见的追溯场景中，物联网感知层通过 RFID[6]等感知技术，将物理物品的属性和状态数据以便捷、低成本的方式通过物联网网络层技术传送到物联网应用层，为物联网应用中的其他相关服务提供关键的数据支持。

物联网应用层追溯服务的典型场景之一是跨组织追溯[7-9]。此处的“跨组织”不仅仅指不同公司、企业之间的相互协作，甚至还表示了同一个公司或企业内部的不同责任群体或环节之间的相互协作[10, 11]。例如对于奶制品供应链来说，一份奶制产品需要经历奶牛农场的生产机构、加工商的检测机构和加工商包装机构、零售商的仓储机构和销售机构等不同的“组织”，才能最终到达顾客的手中。在跨组织追溯场景中，这些不同公司不同责任群体理论上都应当是被追溯的环节。由于跨组织的追溯过程涉及了更多以及更加复杂的机构组织，因而也面临着更严苛的安全挑战。例如当供应链中出现商品损坏等异常时，相关组织可以通过篡改数据以逃避责任且不被发现。因此，跨组织追溯服务面临着严重的安全问题，有待研究和解决。

物联网跨组织安全物品追溯系统中需要同时满足三个基本安全属性:

- **可追溯性**: 是指具有追溯需求的目标用户可以通

**通讯作者 1**：沈烁，博士，副研究员, Email: sean.s.shen@qq.com。**通讯作者 2**：王晓阳，博士，教授, Email: xywangCS@fudan.edu.com。
本课题得到十二五国家密码发展基金(No. MMJJ201301008)，国家自然科学基金(No. 61572136)资助，和 DNSLab 开放课题的支持。
收稿日期：2015-11-28；修改日期：2015-12-21；定稿日期：2016-01-05

过跨组织安全物品追溯模型查询到整条供应链的详细情况。在物联网跨组织安全物品追溯系统的三个安全属性中, 可追溯性是最基本的功能性指标。首先, 在跨组织安全物品追溯服务中, 供应商的信息管理等支持系统需要记录物联网环境中相关物体的基本信息数据和状态改变数据, 如物品产生时特有的属性信息和物品进出某个组织的可信域的状态数据信息等。对数据进行详细且实时地记录是保证物品可追溯性以及追溯质量的重要前提。其次, 在对必要的数据信息进行记录后, 追溯服务还需要给不同角色的用户提供不同的接口, 以呈现不同视角的跨组织追溯信息。在跨组织追溯场景中, 目标用户可大体分为供应商、终端消费者和监管者三种角色, 他们对供应链中物品的状态信息有着不同的需求。

- **可信性**: 是指通过跨组织安全物品追溯系统公开查询到的追溯结果对目标用户是可信的。在物联网跨组织安全物品追溯系统的安全属性中, 可信性是一项关键的安全性指标。实现数据可信性的关键在于保证数据的完整性, 如不被非法篡改。在跨组织追溯场景中, 数据的可信性保护需要一个完善的管理机制以及不同组织之间的合作来实现。
- **隐私保护**: 是指跨组织追溯服务能够根据特定的隐私保护策略保护不同目标角色的隐私数据。在物联网跨组织安全物品追溯系统的安全属性中, 隐私保护是另一项关键的安全性指标。跨组织追溯服务会共享物联网中大量物品的数据信息。然而, 大量的信息共享难免会带来一定程度的私密信息泄露, 其中包括供应商的机密信息和目标用户的隐私信息等。因此, 为了满足跨组织安全物品追溯模型中隐私保护的需求, 参与角色需要制定各自的隐私保护策略[12]。

为满足上述跨组织安全物品追溯中的三个安全属性, 论文形式化定义了跨组织安全物品追溯问题, 提出了实现跨组织安全物品追溯的框架, 同时也实现并评估了跨组织安全物品追溯原型系统。

余下的论文组织如下: 第二部分介绍了相关研究工作; 第三部分形式化定义了跨组织安全物品追溯问题; 第四部分设计了跨组织安全物品追溯框架; 第五部分介绍了系统实现与评估; 第六部分讨论了相关的安全性问题; 第七部分总结全文。

## 2 相关工作

物联网追溯技术强调构建一个虚拟的物流动态信息化互联网管理体系, 同时也重视将 RFID 技术[6]、传感网与现有的互联网整合起来, 通过精细、动态、科学的管理, 实现物流的自动化、可视化、可控化、智能化和网络化, 从而提高资源利用率和生产力水平, 创造综合内涵更丰富的社会价值。

鉴于产品的特性和需求, 追溯技术目前主要应用在安全性能要求较高的产品行业(如: 药品、食品等)和其他高附加值的产品行业(如: 汽车、航天航空器材等)的管理中。除基本的工业应用外, 一些知名的信息技术公司也各自研发了基于物联网的追溯应用。其中, IBM 公司和奥迪公司进行了合作, 设计并研发了“汽车搜索”项目, 实现对汽车产品的实时监控。此外, IBM 还提出了基于食品追溯框架的“智能食品”项目, 以提高食品产品分配流水线的效率、降低食品产品的损坏率。在航天航空领域, 英国剑桥大学的 Auto-ID 实验室一直致力于研究航天航空产品的追溯项目, 旨在将其广泛稳定地应用到航天航空工业中[13, 14]。该项目解决了航天航空产品的几个问题: 产品生命周期管理、零部件的标识符匹配、传感器集成、数据同步等[15-17]。在食品安全领域, Lindsay 提出了一种追踪和监控产品新鲜度和保质期的方法, 该应用会随时监控食品的新鲜度, 并给用户提供过期食品的警告[18]。德国利用产品条码技术, 对其国内的鸡蛋进行统一的食品安全管理。每一个鸡蛋上都有一个红色标码, 消费者可以通过这些标码进一步查询鸡蛋的信息, 按需选择, 如母鸡的饲养方式、鸡蛋的出产国以及母鸡所在的养鸡场和鸡舍的编号。一旦鸡蛋的质量出现了问题, 监管部门可以依据信息一直追查到饲养场或鸡笼。由此可见, 产品的追踪追溯服务不但为消费者详细地了解产品供应链信息提供了便利, 还为监管者更好地监管产品供应链提供了保障。

跨组织物品追溯是物联网追溯服务中更常见且更复杂的场景。目前, 跨组织追溯的相关领域只有一些初步的研究和发展。论文经过大量调研发现, 大部分的跨组织追溯研究重心仍集中在多组织的资源共享和管理上。其中, 虚拟企业访问控制系统 (Virtual Enterprise Access Control, VEAC) 被提出, 以解决在多个组织的虚拟场景中, 各组织之间资源的安全授权、管理和控制问题[19]。虚拟企业访问控制系统的解决方法主要包含了如下四个功能: 企业间信息的安全共享; 工作人员之间的协同合作; 信息透明度的增强; 信息延迟的减弱。此外, 在跨组织的供应链企业管理研究中, 为了更好地协同供应链中各个独立的企业, 虚拟组织 (Virtual Organization, VO) 的

概念被提出。Strader 等人提出了虚拟组织的信息基础架构, 并定义了虚拟组织中关键步骤的生命周期[20]。受益于高速发展的互联网技术和局域网技术, Strader 提出的虚拟组织的信息基础架构可以实现更高效率的信息沟通需求。然而, 虚拟组织最基本的活动和需求是数据的分析和追溯[21]。但大部分的跨组织追溯研究尚停留在不同组织的合作和管理以及系统架构设计上, 并没有充分考虑到用户应用层面的安全物品追溯服务。

综上所述, 物品追溯技术已经在物联网领域有了初步的研究和应用。然而, 随着物联网技术的不断发展, 尤其是价格和用户体验上的改善, 物联网追溯技术越来越深刻地影响当前社会。同时, 它也面临着更为严苛的安全要求和挑战。正如上文所述, 大部分的追溯服务都部署在一个单独的可信域内, 基于跨组织追溯场景的研究仍旧缺乏。

## 3 跨组织安全物品追溯问题

### 3.1 基本定义

在跨组织追溯服务中, 参与者包括三类角色: 供应商、产品的终端消费者和诸如政府职能机构等监督机构。其中, 消费者有需求了解整条供应链, 包括从生产商到终端消费者方向上的详细信息。监督机构更有权从生产商到终端消费者以及终端消费者到生产商两个方向上审查整条供应链。此外, 监督机构还有权查看和统计供应商所提供的商品信息(如质量检测, 销售量等)。

针对以上两个不同的追溯方向, 论文首先介绍系统中所涉及的供应链前向和后向的关系: 一条供应链中, 上游供应商所在的位置被称为下游供应商的后方向, 反之, 下游供应商所在的位置被称为上游供应商的前方向。

论文在定义 1 中初步给出了跨组织追溯模型(*Cross-Organizational Tracking Model, COTM*)的形式化定义。该定义中的模型可以提供最基本的跨组织追溯服务。

**定义 1.** 基本的跨组织追溯模型**:**

$$COTM_{basic} := \{SUBJS, VOS, PRODS, InfoChainS\}$$

其中,

- *SUBJS* 表示跨组织追溯模型中的所有参与者所组成的集合。根据上文所述, 跨组织追溯模型的参与者可分为三类: 供应商、终端消费者和监督机构。
- *VOS* 表示跨组织追溯模型中的虚拟组织的集合。虚拟组织表示一条供应链中涉及的多家供应商所组成的动态组织结构。此外, 虚拟组织的成员通常还是跨组织追溯模型中的参与者, 即 *SUBJS* 集合的元素。下文的定义 2 中, 我们对跨组织追溯模型中虚拟组织的内容进行了形式化地定义。
- *PRODS* 表示流转在跨组织追溯服务中的产品的集合, 也是跨组织追溯模型中追溯服务的追溯目标。对于 *PRODS* 中的每一个产品, 跨组织追溯服务都应提供并保障一个全局唯一标识符 *PID*, 以提供基于 *PID* 的全局追溯服务。
- *InfoChainS* 表示 *PRODS* 集合中产品的信息链。每条信息链包含产品的初始信息段(如产品的初始化参数)和一至若干条嵌套的供应链信息段(如物品离开一个可信域时的发货信息和进入一个新的可信域时的收货信息)。在基于电子履历标准的跨组织追溯系统实现中, 系统使用电子履历文件作为产品信息链 *InfoChainS* 的实例。在定义 3 中, 我们对 *InfoChainS* 中信息链的构成进行了形式化地定义。

**定义 2.** 虚拟组织:

$$VO :=< Leader, 2^{Suppliers} >$$

其中,

- *Leader* 表示一个虚拟组织中的主导公司。每个虚拟组织都包含一系列的供应商和一个主导公司。这个主导公司可能是虚拟组织中的某个供应商, 即 *Suppliers* 中的一个元素, 也可能是一个监督机构或安全联盟。比如, 零售商沃尔玛可以作为主导公司组织一个包含了生产、存储、运输和销售环节的完整的供应链, 食品安全联盟也可以作为主导公司负责监督食品供应链的安全。
- *Suppliers* 表示虚拟组织中的一系列供应商, 它们属于 *SUBJS* 集合的子集。此外, 定义 2 使用了 $2^{Suppliers}$ 来表示供应商 *Suppliers* 的幂集。

**定义 3.** 供应信息链:

$$InfoChain :=< InitInfoSeg | InfoChain, InfoSeg >$$

其中,

- *InfoChain* 表示描述产品供应链详细信息的信息链, 对应于基于电子履历标准的跨组织追溯系统中的电子履历文件的内容。此处, 我们使用了递归的形式对供应信息链进行描述。通常, 供应信息链由一个初始信息段 *InitInfoSeg* 和一至若干条嵌套的供应链信息段 *InfoSeg* 组成。由该定义可知, 最简单的产品供应链由一条初始信息段 *InitInfoSeg* 和一条供应链信息段 *InfoSeg* 组成。而其他更为复杂的产品供应链均为这条最简单的信息链多次嵌套信息段 *InfoSeg* 而得, 即由一条

初始信息段 *InitInfoSeg* 和多条供应链信息段 *InfoSeg* 组成。

- *InfoSeg* 表示产品的供应链信息段, 论文在定义 4 中对其进行了详细地定义。供应链信息段记录了供应链中产品在主要转移环节中的关键信息。比如, 在供应商发货给下游时, 首先供应商会得到该商品当前的供应信息链 *InfoChain*, 然后供应商会创建一个发货类型的供应链信息段 *InfoSeg*, 这个供应链信息段可能包括上游发货供应商的基本信息、下游收货供应商的基本信息、交易数据等。这个新创建出的供应链信息段会嵌套先前的供应信息链 *InfoChain* 而形成一个新的供应信息链 *InfoChain*, 并发送给下游供应商。
- InitInfoSeg 表示产品供应链中的初始产品信息段。初始信息段记录了产品的基本信息, 包括产品标识符、产品编码、批次号、序列号、生产商和初始化日期等信息。

**定义 4.** 供应链信息段:

$$InfoSeg := < IID, TransferInfo, ?TransactionInfo >$$

其中,

- *IID* 表示了供应链信息段的标识符。跨组织追溯框架有需求为供应链信息段提供具有全局唯一性的标识符。在基于电子履历标准的跨组织追溯系统实现中, 供应链信息段的标识符 *IID* 则对应于电子履历文件的履历 *ID*。
- *TransferInfo* 表示在产品转移时, 参与物流传递的 *SUBJS* 集合中的供应商的相关信息。一般情况下, 该元素由发货供应商信息和收货供应商信息组成。
- *TransactionInfo* 表示物流传递过程中产生的交易信息。一般情况下, 该元素包含交易凭证、收据发票等信息。该元素为供应链信息段的可选信息, 不一定存在于每一条信息段中。

## 3.2 安全属性描述

### 3.2.1 可追溯性

跨组织安全物品追溯模型中的可追溯性是指追溯服务的目标用户, 比如终端消费者, 能够正确的查询到整条供应链的详细情况。跨组织安全物品追溯模型需要提供一些查询接口以实现可追溯性。目标用户可以通过在查询接口输入产品的唯一标识符 *PID* 来获得该产品的信息链。如下, 我们形式化地定义了具有可追溯性的跨组织追溯模型:

**定义 5.** 具有可追溯性的跨组织追溯模型:

$$COTM_A := COTM_{basic} \cup \{Query_A\}$$

其中, $Query_A$ 表示获取产品信息链的查询途径。为了更加形象地表示, 我们对其进行了形式化地定义:

$$Query_A : (s : SUBJS \times PID : Identifier) \rightarrow InfoChain$$

其中, $s$ 表示跨组织追溯服务的目标用户, 该元素属于 *SUBJS* 集合, *PID* 是追溯产品的唯一标识符, *InfoChain* 表示追溯到的标识符为 *PID* 的产品信息链。该定义描述了目标用户通过向跨组织追溯模型的查询接口输入产品的标识符, 来获取产品对应信息链的查询过程。

### 3.2.2 可信性

跨组织安全物品追溯模型中的可信性指通过跨组织追溯系统查询到的追溯结果对目标用户是可信的。跨组织安全物品追溯模型可以通过数字签名的技术来保障追溯数据的可信性。在数字签名解决方案中, 数字签名可以附加在定义 3 中的信息链之中, 以保障数据的完整性。如下, 我们在原有信息链定义 3 的基础上, 拓展出了含有数字签名的信息链的形式化定义:

**定义 6.** 签名信息链:

$$SignedInfoChain := < InitInfoSeg|SignedInfoChain, InfoSeg, Signer, Signature >$$

其中,

- *Signer* 表示数字签名的签署者。一般来说, 签署者为 *SUBJS* 集合中的供应商或供应商的签名机构。此外, *Signer* 还可以作为查询标识。
- *Signature* 表示数字签名。该数字签名用来保证 *SignedInfoChain* 的其余部分在之后数据流动中的完整性和可信性。当一个后向链的可信域(即定义中的 *InitInfoSeg*|*SignedInfoChain* 部分)和当前信息段(即定义中的 *InfoSeg* 部分)的可信域不同时, 一个新的数字签名会被创建来确保当前链的信息段 *InfoSeg* 和之前所有的后向信息段的可信性。需要特别指出的是, *InitInfoSeg* 不需要单独进行数字签名认证。存在这一例外的原因是每个初始化的产品操作总是紧跟着一个发货操作, 而这两个操作通常是在同一个可信域之中进行的。综上所述, 一个 *SignedInfoChain* 实例会包含一个初始信息段 *InitInfoSeg* 和至少一个带有数字签名的 *InfoSeg*。*InitInfoSeg* 的完整性可以由更外层的 *InfoSeg* 的可信域签署的数字签名保证。

最后, 我们形式化地定义了具有可信性的跨组织追溯模型, 如下:

**定义 7.** 具有可信性的跨组织追溯模型:

$$COTM_T := (COTM_{basic} \backslash InfoChainS) \cup \{SignedInfoChainS, Query_T\}$$

在该定义中, "\"符号表示"除去"的意思。和基本的跨组织追溯模型 $COTM_{basic}$ 相比, 在具有可信性的跨组织安全物品追溯模型中, 信息链 *InfoChainS* 被签名信息链 *SignedInfoChainS* 代替, 普通查询 $Query_A$ 也被可信查询 $Query_T$ 代替。除了基本的数据结构, $Query_T$ 的功能和 $Query_A$ 的功能相似。同时, 由于 $COTM_T$ 同样支持 $Query_T$ 的功能, 因此, $COTM_T$ 同样满足可追溯性。$Query_T$ 描述了目标用户通过向跨组织追溯模型的查询接口输入产品的标识符, 来获取产品对应可信签名信息链的查询过程。其形式化的定义为:

$$Query_T : (s : SUBJS \times PID : Identifier) \rightarrow SignedInfoChain$$

其中, $s$ 表示跨组织追溯服务的目标用户, 该元素属于 *SUBJS* 集合, *PID* 是追溯产品的唯一标识符, *SignedInChain* 表示追溯到的标识符为 *PID* 的产品信息链。与普通查询不同的是, 跨组织追溯服务会通过公钥证书来验证查询到的产品信息链的完整性, 并将结果反馈给查询者。

### 3.2.3 隐私保护

跨组织安全物品追溯模型中的隐私保护是指跨组织安全物品追溯模型能够根据相应的隐私保护策略保护供应商和消费者的隐私数据。由于消费者可能会通过查询功能 ($Query_T$ 和 $Query_A$) 查询到供应商的隐私信息, 所以, 跨组织追溯服务通常需要为跨组织追溯模型中的不同参与者提供相关的隐私保护机制。如果没有合适的隐私保护机制, 一个终端消费者可能查询到供应链中所有产品的信息链, 同样其他竞争对手也可以查询到。然而, 供应链信息中的有些内容属于供应商的商业机密, 比如谁是销售商某个产品的最大供应商, 这些信息都应当被隐私保护机制所保护。

针对上述场景中可能存在的隐私泄露问题, 论文根据跨组织追溯场景的特点, 定义了两种隐私保护策略: 前向隐私保护策略和后向隐私保护策略。并提供了相应的形式化定义。

- **前向隐私保护策略**: 前向隐私保护策略是指, 当一个目标用户通过跨组织追溯服务获取到信息链时, 它不能获知在它之后发生的追溯数据的具体内容。
- **后向隐私保护策略**: 后向隐私保护策略是指, 当一个目标用户通过跨组织追溯服务获取到信息链时, 它不能获知在它之前发生的追溯数据的具体内容。

**定义 8.** 前向隐私保护策略:

$$\forall s \in (Suppliers): \neg view(s, \forall SignedInfoChain.InfoSeg : InfoSeg.creator \in s.succeeders) \cap \neg view(s, \forall SignedInfoChain.signer : signer.creator \in s.succeeders)$$

定义 8 是指当前的供应商 *s* 不能查看到当前签名信息链 *SignedInfoChain* 中的下游供应商的信息段 *InfoSeg* 和信息段的签名人 *Signer*。这个隐私保护策略能够避免下游的敏感数据被供应商 *s* 可见, 因为供应商可以通过 *Signer* 获得对应的下游供应商也可以通过 *InfoSeg* 获取对应下游供应商的详细信息。

**定义 9.** 后向隐私保护策略:

$$\forall s \in (Suppliers \cup End\_Customers) : \neg view(s, \forall SignedInfoChain.InfoSe : InfoSeg.creator \in s.precedents) \cap \neg view(s, \forall SignedInfoChain.signer : signer.creator \in s.precedents)$$

定义 9 是指当前的供应商 *s* 不能查看到当前签名信息链 *SignedInfoChain* 中的上游供应商的信息段 *InfoSeg* 和信息段的签名人 *signer*。这个隐私保护策略能够避免上游的敏感数据被供应商 *s* 可见, 因为供应商可以通过 *Signer* 获得对应的上游供应商也可以通过 *InfoSeg* 获取对应上游供应商的详细信息。

针对前向和后向隐私保护策略, 论文形式化地定义了具有隐私保护策略的跨组织追溯模型, 如下:

**定义 10.** 具有隐私保护的跨组织追溯模型:

$$COTM_P := COTM_A \cup \{PrivacyPolicyS\}$$

其中, *PrivacyPolicyS* 包括前向隐私保护策略和后向隐私保护策略。

基于上述三种安全属性的定义, 我们提出了同时拥有可追溯性、可信性和隐私保护的跨组织安全物品追溯模型。

**定义 11.** 具有可追溯性、可信性和隐私保护的跨组织安全物品追溯模型:

$$COTM_{ATP} := COTM_T \cup \{PrivacyPolicyS\}$$

在此需要特别指出的是, 隐私保护策略 *PrivacyPolicyS* 此时作用于签名信息链 *SignedInfoChain*。

至此, 我们已用形式化方式表示了四种跨组织追溯模型, 它们之间包含着如下所示的关系:

**命题 1.** 跨组织追溯模型之间的包含关系:

$$COTM_{basic} \subset COTM_A \subset COTM_T / COTM_P \subset COTM_{ATP}$$

如上述命题所示, $COTM_{basic}$ 是这些模型的基本

信息模型。相反, $COTM_{ATP}$ 则是四者中最复杂的信息模型, 它包括了一个跨组织安全物品追溯服务中最多的信息量和功能需求。该命题的提出为物联网应用层跨组织安全物品追溯服务的分步骤实施提供了解决方案和理论基础。现有的大多数追溯系统仅实现了 $COTM_A$, 采用了 EPCglobal 电子履历技术的追溯系统则实现了 $COTM_T$, 但这些和论文提出的 $COTM_{ATP}$ 仍有一定的差距。为此, 论文利用了密码学技术同时保障安全追溯中的追溯数据的可信性和隐私保护, 从而实现了一个 $COTM_{ATP}$ 及其原型系统。

## 4 跨组织安全物品追溯框架

为实现 $COTM_{ATP}$, 跨组织安全物品追溯框架需要遵循以下四项基本原则:

• **平衡可追溯性、可信性和隐私保护**: 论文所设计的跨组织追溯系统需要平衡 3.2 章节中所定义的可追溯性、可信性和隐私保护三项基本安全属性。

• **混合加密解决方案**: 论文所设计的跨组织追溯系统将使用对称加密和非对称加密两种加密方式, 同时实现跨组织追溯的可信性和隐私保护。其中, 对称加密算法将被应用在XML格式的签名信息链的加密功能中; 非对称加密算法将被应用在创建数字签名和加密对称加密所需的会话密钥功能中。此外, 在数字签名解决方案中, 论文研究并应用了群签名技术, 并用群签名方法对信息链进行群数字签名, 以保护数字签名签署者的隐私信息, 从而使跨组织追溯框架满足可追溯性、可信性和隐私保护的需求。

• **虚拟组织的主导公司成为群签名的群管理者**: 论文所设计的跨组织追溯系统将会使用虚拟组织的群概念来进一步实现加密模块的密钥管理和群签名算法。这种虚拟组织群构架符合现代物流的主流群组织形式。虚拟组织中的主导公司需要承担 $COTM_{ATP}$ 中的安全保障, 它需要实施加密解决方案和群签名方案中的管理员操作, 如负责分发加密解决方案和群签名方案中的公私钥对。特殊情况下, 这些功能可能会被虚拟组织的管理员托管给一个权威证书机构 (Certificate Authority, CA) 来承担。总结说来, 虚拟组织的主导公司被认为在具有可追溯、可信性和隐私保护的跨组织安全物品追溯模型中是安全可靠的, 安全保障同时也是虚拟组织主导公司应该承担的责任。

• **使用中央存储方式进行存储和查询**: 论文所设计的跨组织追溯系统使用了中央集中存储的方式。虚拟组织中的供应商和中央存储形成了一个主从式的系统架构。供应商在创建 *SignedInfoChain* 或 *InfoChain* 实例后, 会将它们上传到中央存储处。这样的设计可以更加方便的让用户通过 *PID* 或者 *IID* 进行 *SignedInfoChain* 或者 *InfoChain* 信息的查询。例如, 在基于电子履历标准的跨组织追溯系统实现中, 供应商需要将各自产生的本地电子履历文件上传至中央存储服务器处。然后中央存储就可以通过查询存储的海量电子履历文件和供应商信息, 为跨组织追溯模型中的参与者提供查询接口。

### 4.1 基本框架

图 1 为论文所设计的跨组织安全物品追溯系统的主要成员结构和密钥管理结构。系统主要由以下部分组成:

• **一个安全主导公司 (Secure Leader)**: 安全主导公司在本系统中拥有群签名机制中的群管理员身份以及加解密机制中的密钥持有者身份。因此, 它需要承担保管虚拟组织群密钥对的责任。群密钥对包括了群公钥 ($k_{gpu}$) 和群私钥 ($k_{gpr}$)。其中, 群组织的任何成员可以使用群公钥验证签名信息链 *SignedInfoChain* 中的产品追溯信息, 群组织的管理员可以使用群私钥来获取签名信息链 *SignedInfoChain* 中签名信息的真正签署人, 即反匿名操作。*paramsys* 表示群签名机制需要的参数集合。此外, 主导公司还保管群组织的公钥 ($k_{pu}$) 和私钥 ($k_{pr}$) 对。这组密钥的功能是保护主导公司和每个供应商之间的通讯安全以及对 *SignedInfoChain* 中的商业数据加密。

• **多个供应商(Suppliers)**: 如图 1 所示, $s_1$ 到 $s_n$ 均表示虚拟组织中的供应商, 这些供应商属于定义 2 中的 *Suppliers* 集合。在签名方案中, 这些供应商需要各自保管一个主导公司分发的群签名私钥 ($k_{spri}$)。需要特别指出的是, 主导公司可以知道群中所有成员的签名私钥。此外, 每个供应商都拥有一个独自的存储空间, 该空间用于存储供应商创建的 *SignedInfoChain* 实例。例如, 在基于电子履历的跨组织安全物品追溯模型中, 每个供应商有各自的存储数据库来存储自己创建的本地电子履历文件。

• **一个中央存储**: 正如设计原则中所描述, 中央存储模块负责存储所有供应商创建的签名信息链 *SignedInfoChain* 实例, 方便为用户统一提供追溯这些数据的接口。

• **海量追溯数据实例**: 即为形式化定义中的签名信息链 *SignedInfoChain* 的实例。追溯数据实例由供应商创建, 后可以被创建者存储, 也可以被创建者上传至中央存储模块。在基于电子履历的跨组织追溯框架中, 电子履历文件是一种追溯数据实例, 我们称之为隐私保护增强电子履历文件。

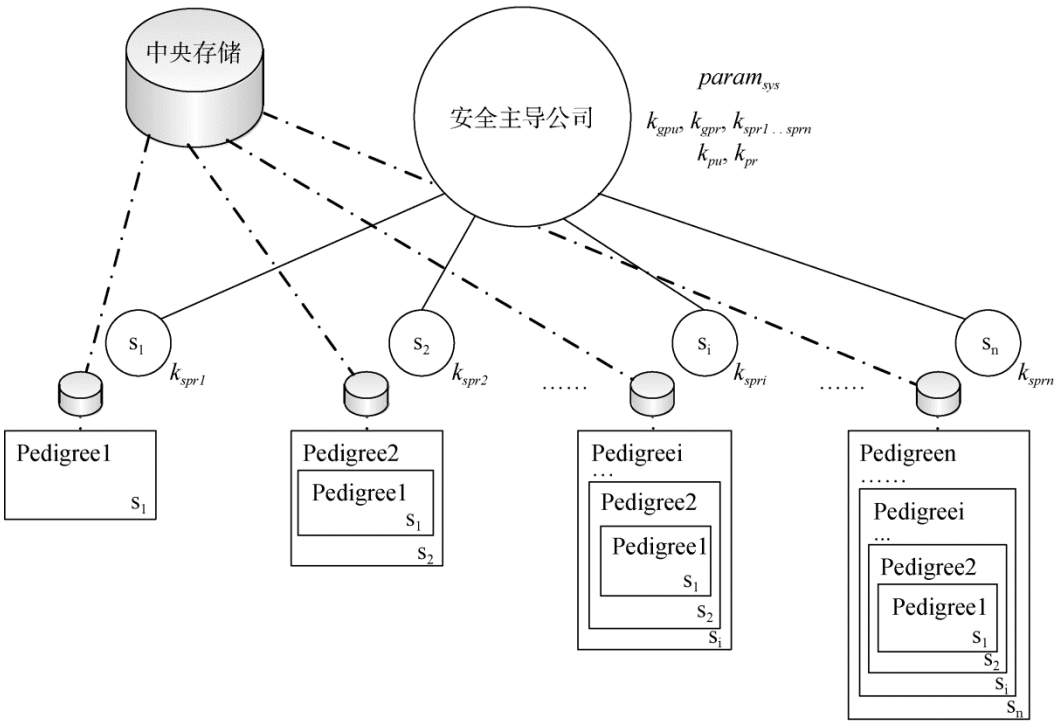



**图 1　基于群签名的跨组织安全物品追溯系统加密模块的主要构成**

## 4.2　跨组织物品追溯协议簇

在典型的供应链场景中, 发货和收货是两个核心的操作流程, 它们是产品所在的可信域转移的必然过程。其中, 发货过程意味着产品从一个供应商可信域离开, 并转移到它的下游供应商可信域。反之, 收货过程意味着供应商接受来自上游商家可信域的产品, 并使产品进入到自身可信域。除此之外, 当供应商接收到产品时, 还需要验证来自上游商家的产品签名信息链。因此, 在论文提出的支持 $COTM_{ATP}$ 的实现系统中, 关键的三个协议为发货协议、验证协议和收货协议。

### 4.2.1　发货协议

发货协议的主要目的是加密发送者的详细信息, 以及对信息链 *SignedInfoChain* 实例中的信息进行群签名。其中, *SignedInfoChain* 实例论文会以隐私保护增强电子履历的形式详细介绍。在商品发货后, 发货协议可以保障生产线下游商家无法从已被签署的隐私保护增强履历文件中获得或者修改发货者的详细信息。这种加密操作可以帮助跨组织追溯系统实现隐私保护策略中的后向隐私策略。同时也可以实现前向隐私策略。

图 2 为基于电子履历系统实现的跨组织安全物品追溯框架的发货协议图。当前的供应商首先会使用会话密钥对电子履历发货人信息和可选的当前供应商交易进行加密(如 AES 加密)。此外, 供应商还可以使用会话密钥加密除初始信息段之外的旧签名信息链。需要强调的是, 初始信息段不会被加密。这是因为初始信息段中包含一些诸如产品编码等基本产品信息, 而这些基本信息包含 $Query_T$ 操作的主要查询属性, 明文存储有利于提高跨组织追溯查询的性能。

在发货和收货的信息加解密过程中, 会话密钥是关键组成元素, 其具有以下的特点:

- **机密性**: 会话密钥用于隐私保护增强电子履历信息的对称加密, 而会话密钥本身也会被供应商使用非对称加密存储。在发货协议环节中, 会话密钥会被群主导公司的公钥进行加密并附在隐私保护增强电子履历文件中。因此, 只有群主导公司可以使用群私钥来查看加密内容。
- **随机性**: 每一次的发货协议中, 会话密钥都是在所有的 AES 加密操作前随机生成的。
- **相同协议中的重用性**: 在同一次的发货协议中, 如图 2, 不同的属性都使用同一个会话密钥进行加密。
- **不同协议中的一次性**: 在每一次的发货协议中, 即使是同一个供应商发货, 产生的会话密钥也是不同的, 如图 2 所示, 当前供应商部分的会话密钥和上游供应商的会话密钥是不相同的。因此, 查看隐私保护增强电子履历的所有加密内容需要虚拟组织的主导公司进行一层一层的解密。

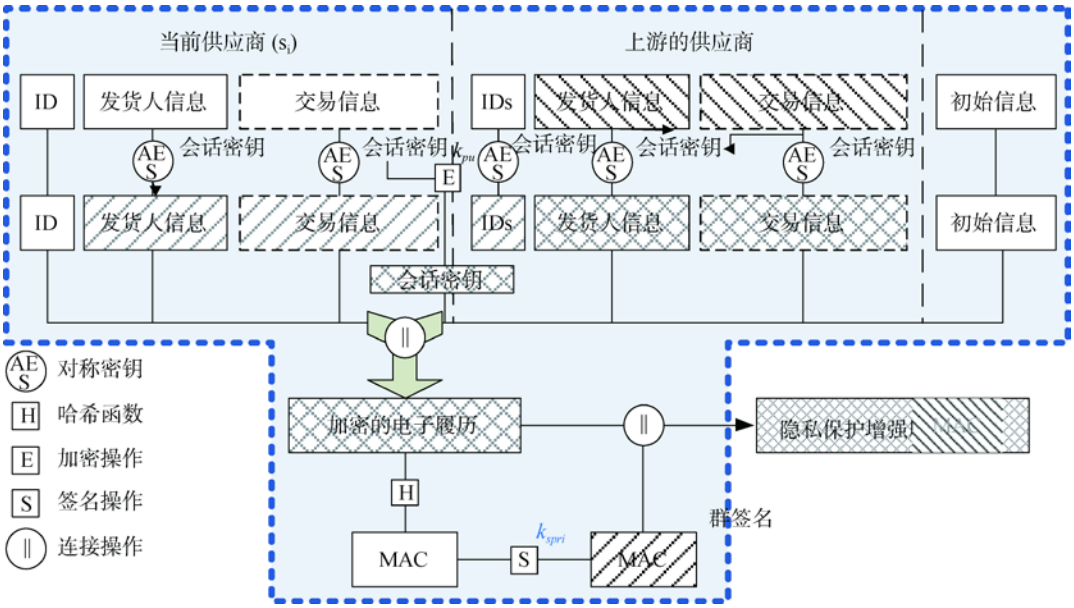



**图 2　发货协议图**

• **多次加密机制**: 上游供应商的信息到达当前供应商时即使已被加密，在本次发货协议中仍需要再次加密。这样可防止在一次解密后，解密者根据密文明文对比获得其他产品的供应链信息。

加密之后，供应商会重新组织电子履历文件中的信息，并形成如图 2 所示的电子履历组成，我们用阴影框中“加密的电子履历”表示。然后，供应商使用特定的哈希函数(图中字母 H 所示)，比如 SHA256，创建消息验证码 (*MAC*)，并使用供应商持有的签名私钥对其进行群签名。最后，签名和加密的电子履历组合成为一个隐私保护增强的电子履历然后被发送到供应商的下游。

供应商下游的商家只能通过群公钥来验证隐私保护增强电子履历的合法性。并且，该商家只能查看到此电子履历文件的标识符 (*ID*) 和产品的初始信息等不被加密的公开信息。其他隐私信息则只能通过虚拟组织的安全主导公司进行解密获得。

综上所述，由于发货协议需要加密每一层的签名信息链。因此，发货协议的理论时间复杂度为 O(n)，其中 n 表示签名信息链的数目，即隐私增强电子履历文件的嵌套层数。

### 4.2.2　验证协议

验证协议的主要目的是帮助使用者验证供应商或其他群成员签署的 SignedInfoChain 实例是否合法，即验证隐私保护增强电子履历是否完整、是否由群成员进行签署。

隐私保护增强电子履历的验证协议如图 3 所示。根据发货协议的介绍可知，隐私保护增强电子履历

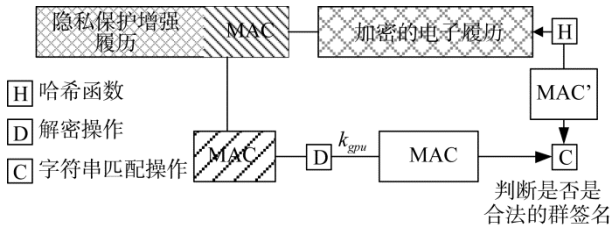



**图 3　验证协议**

由加密的电子履历和被签名的消息验证码 (*MAC*) 两个部分组成。验证者首先使用和发货协议相同的哈希函数创建一个新的消息验证码 (*MAC'*)。然后，使用群公钥解密隐私保护增强履历中携带的消息验证码 (*MAC*)，并将其与新的消息验证码 (*MAC'*) 进行对比。如果原来的消息验证码和新的消息验证码相同，则该隐私保护增强履历是由一个群成员合法签名的(同时可以确保验证者无法知晓签名者的具体成员身份)并且它未被篡改。反之，则该隐私保护增强电子履历不是被群成员签名的或者其完整性已被破坏。

普通群成员可以通过验证协议验证签名的合法性，群主导公司在确认隐私保护增强电子履历文件是由群成员签名之后，可以使用自己持有的群私钥 ($k_{gpr}$) 和群成员签名私钥记录 (记录了供应商 $s_i$ 和签名私钥 $k_{spri}$ 的对应记录表) 打开签名，即反匿名操作，从而得知签署人员的具体成员身份。

由于电子履历文件的验证环节需要验证每一层嵌套 XML 电子履历的数字群签名，因此验证环节的时间复杂度为 O(n)，其中 n 表示电子履历文件的嵌套层数。

### 4.2.3　收货协议

收货协议的目的在于验证收到的隐私保护增强

电子履历文件的数字签名, 同时附上收货者的信息, 并对新的隐私保护增强电子履历进行数字签名。和发货协议一致, 为了确保隐私保护策略的实现, 收货者的信息会在数字签名前进行加密。

如图 4 所示, 当前供应商收到的隐私保护增强电子履历文件包括两部分, 加密履历和签署的消息验证码 (*MAC*)。和验证协议相同, 收货者首先使用和发货者相同的哈希函数创建一个和收到的加密电子履历相关的新消息验证码 (*MAC'*)。然后通过对比原来的消息验证码与新的消息验证码来判断该隐私保护增强履历是否由一个合法群成员签名以及它是否被修改。

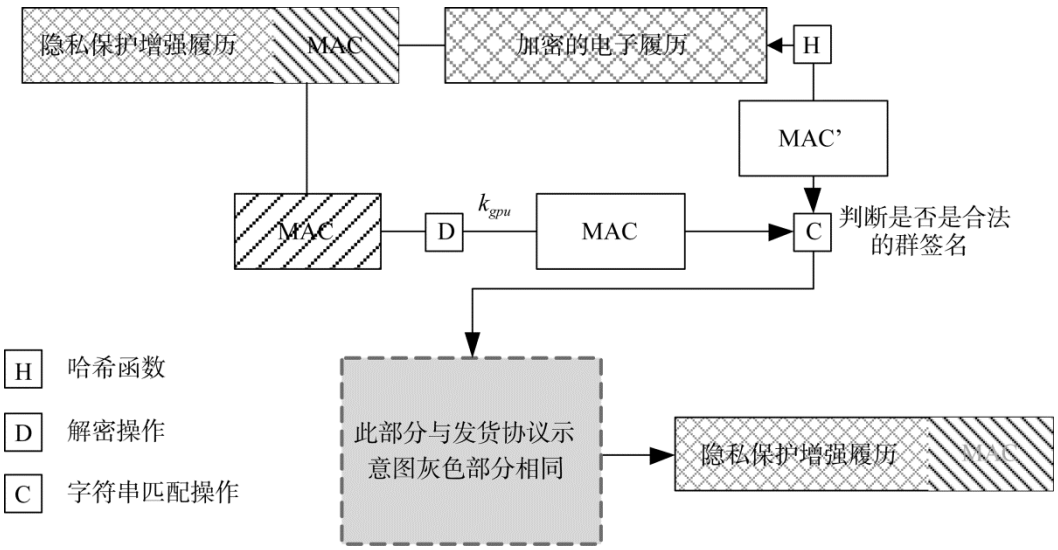



**图 4 收货协议**

收货协议中, 电子履历验证后的其他过程和发货协议相似。收货者随机生成新的会话密钥, 并使用新的会话密钥加密收货者信息、可选的交易信息和签名信息链的旧信息段。然后, 新的会话密钥会通过群公钥进行加密。两个加密过程均完成后, 收货者按照加密履历的格式重新组织电子履历文件, 并使用哈希函数创建消息验证码 (*MAC*), 然后使用收货供应商的群签名私钥对消息验证码签名。最后, 新的签名和加密履历组成新的隐私保护增强履历。

尽管收货协议操作只在旧的电子履历文件中增加了小部分的数据块, 它仍需要进行类似于验证协议和发货协议的流程。收货协议需要验证每一层的签名信息链, 还需要再次加密每一层的签名信息链。因此, 收货协议的时间复杂度为 O(n) , 其中 n 表示电子履历文件的嵌套层数。

## 5 原型系统与评估

论文所实现的原型系统部署在两台惠普 p7 的服务器上。两台机器均拥有四核的 Intel Core i5-2500S 处理器和 4GB 的内存, 其中处理器的主频为 2.70GH。两台服务器的操作系统为 Windows 7 企业版。原型系统使用版本为 3.6 的 Eclipse 和版本为 1.6.0 的 JAVA 语言进行开发。一台服务器用于部署群安全主导公司, 另外一台服务器用于部署供应商的相关服务。

在性能评估阶段, 论文设计了相应的性能评估试验, 分别将供应商的数量设置为 10、20、50 和 100 个, 并分别多次运行了论文设计的跨组织安全物品追溯框架 $COTM_{ATP}$ 中的关键流程。在性能评估试验中, 论文使用了 SHA256 算法作为生成消息验证码 (*MAC*) 的哈希函数, 因此, 在本试验中, 消息验证码 (*MAC*) 固定为 256 比特的长度。为了使评估结果更加准确, 我们运行了 100 遍相同的试验内容, 并采用试验结果的平均值。表 1 显示了试验结果。其中, 签名和验证均使用了单层嵌套的隐私保护增强电子履历文件作为目标。

**表 1 不同供应商数量下的关键流程性能评估**

| 供应商数量 | 10 | 20 | 50 | 100 |
|---|---|---|---|---|
| 生成系统参数 (ms) | 250 | 282 | 250 | 266 |
| 生成公私钥对 (ms) | 93 | 93 | 78 | 78 |
| 生成供应商私钥 (ms) | 25 | 28 | 25 | 25 |
| 签名 (ms) | 327 | 359 | 329 | 327 |
| 验证 (ms) | 359 | 392 | 359 | 359 |
| 反匿名 (ms) | 422 | 438 | 421 | 405 |

根据表 1 所示的实验结果, 当供应商数量不同时, 主要的公私钥操作并没有显著的性能差异。其中,

生成相应的系统参数所需的时间在 266±6%ms 范围内; 生成群公钥 ($k_{gpu}$) 和群私钥 ($k_{gpr}$) 所需的时间在 85.5±7%ms 的范围内; 生成每个供应商群签名私钥 ($k_{spri}$) 的时间在 26.5±6%ms 范围内; 群签名签署操作所需的时间在 375.5±4.4%ms 范围内; 群管理员进行反匿名操作的时间在 421.5±3.9%ms 范围内。该试验表明了论文所提出的跨组织安全物品追溯框架 $COTM_{ATP}$ 在实际应用中有效可行。

在参考文献[22]和[23]中, 作者同样提出了一种新的方法来验证并保护基于 RFID 的商品供应链。该方法使用多项式方法对标签在供应链中的有效路径进行编码记录, 同时读写器可以通过标签中记录的路径对产品进行验证。上述文章中的 Tracker 机制[22]和 Checker[23]机制通过 RFID 标签对产品路径进行可信性和有效性保障, 不同的是, 论文所提出的跨组织安全物品追溯框架设计并保护了供应商所记录的所有商业数据信息。另外, Tracker 机制和 Checker 机制运行在物联网传感器层, 而我们提出的跨组织安全物品追溯框架运行在物联网的商业应用层, 具有更好的用户体验。此外, 由于 Tracker 机制和 Checker 机制的实施依赖于 RFID 标签和传感器进行标签数据存储和读取, 相比之下, 论文所提出的跨组织安全物品追溯系统仅依赖于 XML 文件进行数据存储的方法具有更好的拓展性、兼容性和易用性。

论文也分别对比了其他两个应用层实现方案: SecTTS 系统[24]和农产品电子履历系统[25]。如表 2 所示, 我们针对论文所提出的跨组织安全物品追溯系统中的可追溯性、可信性和隐私保护三个安全属性, 对这三个系统进行了横向对比。其中, 我们将隐私保护分类为前向隐私保护、后向隐私保护和供应链的不可链接性。该表中, 我们使用“√”和“×”符号分别来表示一个系统是否满足相应的安全属性。

**表 2 基于安全属性的应用层方案对比**

| 安全属性 | $COTM_{ATP}$ | SecTTS | 农产品电子履历系统 |
|---|---|---|---|
| 可追溯性: | √ | √ | √ |
| 可信性: | √ | × | √ |
| 隐私保护: | | | |
| 前向隐私 | √ | √ | × |
| 后向隐私 | √ | √ | × |
| 不可链接性 | √ | × | × |

首先, 我们对比了 SecTTS 系统和论文提出的跨组织安全物品追溯框架 $COTM_{ATP}$。如表 2 所示, SecTTS 系统并没有使用任何完整性保护方法来保障商业数据的可信性。这就意味着, SecTTS 系统所提供的追溯数据可能在任何一个传输阶段被未授权的更改; 此外, 在隐私保护方面, 虽然 SecTTS 系统保障了供应链的前向隐私和后向隐私, 但是在供应链的不可链接性的保护方面有所不足。

然后, 我们又将农产品电子履历系统和论文的跨组织安全物品追溯框架 $COTM_{ATP}$ 进行了对比。如表 2 所示, Han 提出的农产品电子履历系统仅考虑了跨组织追溯场景中商业数据和产品数据的可追溯性和可信性。然而, 这个为食品安全考虑的系统却并不能够保证系统的前向隐私安全、后向隐私安全和供应链的不可链接性。相比之下, 论文所设计的跨组织安全物品追溯框架可以同时满足可追溯性、可信性和隐私保护三个安全属性。

## 6 讨论

论文提出的跨组织安全物品追溯框架满足了可追溯性、可信性和隐私保护三项基本安全属性。此外, 它还可能会承受以下的一系列安全挑战。

- **供应商的共谋攻击**: 由于供应商可以从自己的商业管理体系(如 EPCIS、ERP 系统)中获取到自己生产线直属上游和下游的供应商信息。如果攻击者可以聚合大量的供应商所持有的信息, 便有可能拼凑出完整的供应链信息。这些信息并不是从论文提出的跨组织安全物品追溯系统所设计的隐私保护增强电子履历中泄露, 而是从供应商各自的商业信息管理体系中泄露。因此, 仅仅依靠隐私保护增强电子履历并不能很好地解决供应商利用其它管理系统的共谋攻击。
- **使用已解密的密文来映射密文电子履历**: 当生产线下游的供应商收到一份商品的电子履历文件后, 可以得到该产品的签名信息链, 该信息链由部分加密的敏感机密信息、部分明文信息和数字签名组成。如果在此之前, 恶意的供应商从虚拟组织主导公司处获得了先前加密信息的对应明文形式, 它将会获得一系列有效的密文和明文的对应关系。因此, 存在这样一种攻击方式, 恶意供应商通过已有的密文明文对应关系, 直接对应得到其他供应商并没有权限解密的电子履历机密信息。但是, 由于发货协议和收获协议中, 所有待加密的机密信息均使用会话密钥进行加密。同时, 由于不同的供应商和不同的协议环节在加密电子履历文件时均使用不同且随机生成的会话密钥, 因此, 理论上不同的供应商无法获得有效的同一会话密钥下的密文明文对。比如, 一个恶意的供应商获得了一个加密的电子履历文件, 该电子履历文件使用了会话密钥 A, 同时该供应商有权限从虚拟组织的主导公司处获得该加密文件对应

的明文形式。然后该供应商便可获得一个会话密钥 A 的密文明文对应表。例如，供应商从第一个履历文件元素中读取元素“产品序列号”的密文为“αβγ”，因此，该恶意供应商便可对应起所有的密文为“αβγ”的产品序列号的值。然而，由于每个不同供应商的发货协议中使用的加密会话密钥不同，因此，在其他的电子履历文件中，该密文明文对是无效的。综上所述，论文设计的跨组织安全物品追溯框架可以很好地应对已解密密文和明文的对应攻击。

- **群成员签名私钥的撤回**：在论文提出的跨组织安全物品追溯框架中，一旦某个供应商的签名私钥泄露了并被攻击者获得，那么该攻击者可以使用该签名私钥对任何的信息进行签名。由于该签名私钥是合法有效的，因此，攻击者所签署的任何信息都会被虚拟组织认证为合法的。此后，攻击者可以肆意的利用此漏洞来签署错误的信息。为避免更多的攻击，此种攻击一旦被汇报，安全主导公司便会采取相关措施。其中一种解决措施是更新包括群公钥、群私钥、供应商签名私钥等所有的公私钥对。然而，对于虚拟组织的安全主导公司来说，更新整个群的公私钥对是非常复杂的操作。因此，如何降低群签名私钥撤销的复杂度也是如今非常热门的研究课题。论文暂时无法实现避免更新整个群公私钥对的签名私钥撤销方式。
- **公钥基础设施(PKI)的自身缺陷**：论文所提出的多项协议和追溯框架都是建立在公钥基础设施(PKI)的安全性基础上的。因此，几乎所有的公钥基础设施的缺陷都存在于论文的跨组织安全物品追溯框架和相关协议中。一旦群组织成员的签名私钥或者群私钥遭到泄露，整个框架和协议的安全性都会被打破。除此之外，会话密钥和加密算法也都是论文的跨组织安全物品追溯框架和协议的关键安全元素。一旦系统所使用的对称加密、非对称加密、群签名算法的安全性受到破坏，系统的安全性也会大大降低。
- **单点故障缺陷**：论文所提出的跨组织安全物品追溯框架是一个主从式架构的框架，该框架由一个安全主导公司和许多供应商组织组成。然而，系统中部分关键的操作，如签名的反匿名化、信息的解密、追溯数据的存储和查询都集中在安全主导公司这一个可信点上的，因此，本系统存在单点故障的缺陷。但是，本系统可以采取一些常见单点故障缺陷的解决方案进行缓解，如冗余备份。一方面海量的储存数据在不同的供应商处有分布式的备份，另一方面安全主导公司处也可以提供其他密钥管理相关的备份服务器。这些可以从一定程度上缓解单点故障给系统带来的负担和损失。

## 7 结论和展望

论文针对物联网跨组织追溯场景中的数据安全问题，提出并定义了三项基本安全属性：可追溯性、可信性和隐私保护，定义了满足这三个属性的跨组织安全物品追溯模型，并实现了满足该模型的隐私保护增强电子履历原型系统。此外，针对安全属性中的隐私保护，论文还定义了两种隐私保护策略：前向隐私策略和后向隐私策略。根据调研，本文是首个同时提出并解决以上三个跨组织追溯模型中安全问题的研究。根据论文中的评估，论文提出的跨组织安全物品追溯模型满足跨组织安全物品追溯服务的三个安全属性，且在现实应用中具有可以接受的性能。

在将来的工作中，我们拟优化跨组织安全物品追溯模型，深入分析跨组织物品追溯协议簇的安全性，最后推动跨组织安全物品追溯模型和协议簇在实际系统中的应用。

**致　谢** 本文是复旦大学硕士毕业论文“基于物联网的跨组织安全物品追溯技术与系统研究”的学术论文版本。

## 参考文献

[1] S. Chalasani, R. V. Boppana, “Data Architectures for RFID Transactions,” *IEEE Transactions on Industrial Informatics*, vol. 3, no. 3, pp. 246-257, 2007.

[2] Pedigree Ratified Standard EPCglobal. 1.0., EPCglobal, 2007.

[3] Yun Gu, Weili Han, Lirong Zheng, and Bo Jin, “Using iot technologies to resolve the food safety problem–an analysis based on chinese food standards,” *Web Information Systems and Mining*: *Springer*, pp. 380-392, 2012.

[4] Ovidiu Vermesan, Peter Friess, “Internet of Things-Global Technological and Societal Trends from Smart Environments and Spaces to Green ICT,” *River Publishers*, 2011.

[5] Da Xu Li, He Wu, and Li Shancang, “Internet of Things in Industries: A Survey,” *Industrial Informatics, IEEE Transactions*, vol. 10, no. 4, pp. 2233-2243, 2014.

[6] R. Want, “An Introduction to RFID Technology,” *Pervasive Computing, IEEE*, vol. 5, no. 1, pp. 25-33, 2006.

[7] Zhibo Pang, Qiang Chen, Weili Han, and Lirong Zheng, “Value-centric design of the internet-of-things solution for food supply chain: value creation, sensor portfolio and information fusion,” *Information Systems Frontiers*, vol. 17, no. 2, pp. 289-319, 2012.

[8] G. M. Gaukler, “Item-Level RFID in a Retail Supply Chain with Stock-Out-Based Substitution,” *Industrial Informatics, IEEE Transactions*, vol. 7, no. 2, pp. 362-370, 2011.

[9] T. Inaba, “Technical issues of electronic pedigree inter-organizational transactions,” *Drug Security Network–White Papers*, 2005.

[10] Da Xu Li, “Enterprise Systems: State-of-the-Art and Future Trends,” *Industrial Informatics, IEEE Transactions*, vol. 7, no. 4,

pp. 630-640, 2011.

[11] W. U. Jing, L. I. Qing, and LIU Yong-qing, “A business process-oriented heterogeneous systems integration platform,” *Manufacturing Automation*, 2010.

[12] Weili Han, Chang Lei, “A survey on policy languages in network and security management,” *Computer Networks*, vol. 56, no. 1, pp. 477-489, 2012.

[13] Thomas Kelepouris, Tom Baynham, and Duncan McFarlane, “Track and trace case studies report,” *Aerospace-ID Technologies White Paper Series*, 2006.

[14] Thomas Kelepouris, Samuel Bloch, and Da Silva, “Automatic ID Systems: Enablers for Track and Trace Performance.” *Aerospace-ID Technologies White Paper Series*, 2006.

[15] Jeff Baur, Edward Silverman, “Challenges and opportunities in multifunctional nanocomposite structures for aerospace applications,” *MRS bulletin*, vol. 32, no. 04, pp. 328-334, 2007.

[16] Mark Harrison, Ajith Kumar Parlikad, “Lifecycle ID and lifecycle data management,” *AUTO-ID Labs, AEROID-CAM-005*, 2006.

[17] Mark Harrison, “EPC Identifiers for aerospace,” *Aerospace ID Technologies Programme: White Papers*, 2006

[18] Jeff Lindsay, Walter C. Reade, “RFID system and method for tracking food freshness,” *Google Patents*, 2006.

[19] Tsung-Yi Chen, Yuh-Min Chen, Chin-Bin Wang, Hui-Chuan Chu, and Huimei Yang, “Secure resource sharing on cross-organization collaboration using a novel trust method,” *Robotics and Computer-Integrated Manufacturing*, vol. 23, no. 4, pp. 421-435, 2007.

[20] Troy J. Strader, Fu-Ren Lin and Michael J. Shaw, “Information infrastructure for electronic virtual organization management,” *Decision support systems*, vol. 23, no. 1, pp. 75-94, 1998.

[21] Omar Khalil, Shouhong Wang, “Information technology enabled meta-management for virtual organizations,” *International Journal of Production Economics*, vol. 75, no. 1, pp. 127-134, 2002.

[22] Erik-Oliver Blass, Kaoutar Elkhiyaoui, and Refik Molva, “Tracker: Security and Privacy for RFID-based Supply Chains,” in *Proc. Network and Distributed System Security Symposium (NDSS 2011)*, 2011.

[23] Kaoutar Elkhiyaoui, Erik-Oliver Blass, and Refik Molva, “CHECKER: On-site checking in RFID-based supply chains,” in *Proc. ACM conference on Security and Privacy in Wireless and Mobile Networks (WISEC’12)*, pp. 173-184, 2012.

[24] Jie Shi, Yingjiu Li, Wei He, and Darren Sim, “SecTTS: A secure track & trace system for RFID-enabled supply chains,” *Computers in Industry*, vol. 63, no. 6, pp. 574-585, 2012.

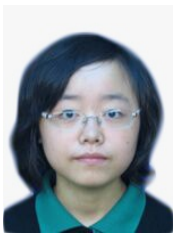
[25] Weili Han, Yun Gu, Wei Wang, Yin Zhang, Yuliang Yin, Junyu Wang, Lirong Zheng, “The Design of an Electronic Pedigree System for Food Safety”, *Information Systems Frontiers*, 2015, 17(2): 275-287.

[26] Liangxing Liu, Weili Han, Tao Zhou, Xinyi Zhang. SCout: Prying into Supply Chains via a Public Query Interface, IEEE Systems Journal, (DOI: 10.1109/JSYST.2014.2337519), 2014.

**韩伟力** 于 2003 年在浙江大学计算机科学与技术专业获得博士学位。现任复旦大学软件学院副教授、副院长。研究领域为网络和系统安全。研究兴趣包括: 访问控制、数字身份管理、物联网安全。
Email: wlhan@fudan.edu.cn.

**王蔚** 于 2015 年在复旦大学计算机软院与理论专业取得硕士学位。研究领域为物联网安全追踪追溯, 移动端安全等。
Email: 12212010019@fudan.edu.cn.

**张胤** 于 2015 年在复旦大学计算机软件与理论专业获得硕士学位。现任 PayPal 单位风控工程师。研究领域为风控、信息安全。研究兴趣包括: 物联网。
Email: 12212010029@fudan.edu.cn.



**袁琅** 于 2014 年在复旦大学软件工程专业获得学士学位。现在在复旦大学计算机软件与理论专业攻读硕士学位。研究兴趣包括: 口令安全和系统安全。
Email: 14212010026@fudan.edu.cn.

**沈烁** 于 2007 年在美国 Purdue University 毕业, 获得数学博士、电子与计算机工程硕士。现在国家物联网标识管理公共服务平台任副主任和 CTO, 中国科学院计算机网络信息中心物联网中心副主任, 中科院副研究员。研究领域为物联网。研究兴趣包括: 物联网标准体系、信息安全等。
Email: shenshuo@niot.cn.

**王晓阳** 于 1992 年在美国南加州大学获得计算机科学博士学位, 1992 年起在美国乔治梅森大学任助理教授及副教授, 2003 年起在美国佛蒙特大学任计算机科学系冠名讲席教授, 2009 年起全职借调于美国国家科学基金会(NSF)任 Program Director, 2011 年到复旦任职。现任复旦大学特聘教授、博士生导师、复旦大学计算机科学技术学院院长。主要研究和授课兴趣包括数据库、并行式数据分析和信息安全。曾主持多项 NSF 以及其他项目, 发表过 100 余篇学术论文, 曾获得 NSF 的 CAREER Award。
Email: xywangCS@fudan.edu.cn.