(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105681306 A
(43)申请公布日 2016.06.15

(21)申请号 201610029898.4

(22)申请日 2016.01.13

(71)申请人 华北水利水电大学
地址 450045 河南省郑州市北环路36号华北水利水电大学

(72)发明人 许德合 张俊峰 杨成杰 赵东保

(74)专利代理机构 北京国坤专利代理事务所（普通合伙） 11491
代理人 姜彦

(51)Int.Cl.
H04L 29/06(2006.01)

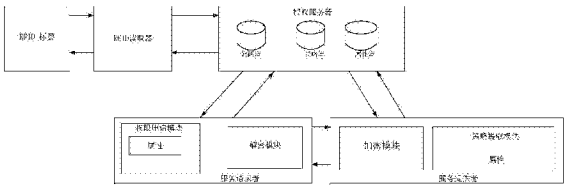
权利要求书5页 说明书18页 附图3页

(54)发明名称

一种基于访问模式保护的空间数据安全控制系统

(57)摘要

本发明公开了一种基于访问模式保护的空间数据安全控制系统，包括授权服务器、服务提供者、服务请求者、射频识别(RFID)读取器和RFID标签。本发明提供的授权服务器模块包括了密钥库、属性库、策略库三部分，密钥库保存了服务请求者的授权公钥和服务提供者的加密私钥，属性库存储系统各方的属性信息，策略库存储系统的决策策略，密钥库、属性库、策略库均具备对保存信息进行增加、删除、查找、备份等基本功能，有效满足了访问控制过程中对信息源的要求，服务提供者的加密处理操作将策略隐含在加密密钥中，蕴含了对资源设定的访问控制规则，同时数据安全也得到了有效的保护。



CN 105681306 A

1.一种基于访问模式保护的空间数据安全控制系统，其特征在于，该基于访问模式保护的空间数据安全控制系统包括授权服务器、服务提供者、服务请求者、RFID读取器和RFID标签；所述授权服务器分别与服务请求者和服务提供者进行数据交互，所述服务请求者和服务提供者进行数据交互；

所述RFID读取器包括电子组件，该电子组件使该RFID读取器能够生成射频场，并与位于该射频场内的RFID装置交换数据；RFID标签信号连接所述RFID读取器，所述RFID读取器与授权服务器信号连接；

所述授权服务器对服务请求者授权指派，对服务请求者和服务提供者提供双方的公私密钥分发，并将安全域访问控制过程和隐私保护机制进行融合；所述授权服务器包括密钥库、属性库和策略库；

所述密钥库用于保存服务请求者的授权公钥和服务提供者的加密私钥；所述属性库存储服务提供者模块和服务请求者模块的属性信息；所述策略库用于存储系统的决策策略；密钥库、属性库、策略库均具备对保存信息进行增加、删除、查找、备份功能；

所述服务提供者是按权限集合的规定接受主体访问的被动实体，所述服务提供者包括策略提取模块和加密模块；

所述策略提取模块通过发送客体属性进行策略提取；所述加密模块负责完成信息的加密工作，包含对资源设定的访问控制策略；

所述服务请求者是对服务提供者拥有使用权限的主动实体，包括授权申请模块和解密模块；

所述授权申请模块通过发送主体属性进行权限申请；所述解密模块负责完成信息的解密工作；

所述RFID标签包括天线和存储器，所述RFID标签被配置为具有通过NFC装置向其存储器写入的加密私钥，并且其中所述RFID标签进一步被配置为通过所述NFC装置向所述RFID读取器传递向其存储器写入的加密私钥；

所述RFID读取器还包括外壳，并且其中所述RFID标签位于该外壳内，向所述RFID标签的存储器写入的加密私钥被存储其中达到预定数量的时间，并然后被删除；

所述RFID读取还包括天线，所述RFID标签的天线中心相对于所述RFID读取器的天线中心偏移，所述RFID读取器进一步被配置为命令所述RFID标签的控制电路将所述RFID标签的天线从所述RFID标签的集成电路脱离达到预定数量的时间，所述RFID读取器经由所述RF场和服务接口中的至少一个向所述RFID标签提供电力；

所述NFC装置，包括处理器，所述处理器包括NFC模块的存储器和NFC接口，所述NFC模块被配置为确定所述NFC装置位于RFID读取器所产生的RF场内，并且响应于确定所述NFC装置位于所述RFID读取器产生的所述RF场内，向也位于所述RF场内的所述RFID标签写入访问控制加密私钥，使得所述RFID标签能代表所述NFC装置向所述RFID读取器传递所述访问控制加密私钥；

所述的NFC装置，还包括使所述NFC装置能够接收该访问控制加密私钥的网络接口，所述NFC模块进一步使所述NFC装置在向所述RFID标签传递所述访问控制密钥之后，能够从所述RFID标签读回信息，从所述RFID标签读回的信息经由所述网络接口传送到中央系统。

2.一种如权利要求1所述基于访问模式保护的空间数据安全控制系统的RFID读取器识

别概率最优树型跳跃协议的方法，其特征在于，所述RFID读取器识别概率最优树型跳跃协议的方法包括以下步骤：数目估算、计算最优跳转层、数目重估、寻找跳频目的地；

首先估计出标签规模，然后根据标签规模，计算最优的树遍历层数以便使预期查询数最小，直接跳跃到那一层的最左节点；

然后在那个节点的子树的执行DFT；

经过对子树的遍历，估算剩下的没有被识别的标签规模，重新计算新的最优层数，直接跳跃到最优节点，并在那个节点的子树上执行DFT，直到所有的节点被识别出结束；

所述数目估算，TH算法首先使用基于帧时隙Aloha的方法快速估算标签数量规模；

所述计算最优跳转层，确定最优层次即TH算法直接跳转到的层次 γ_{op}；

所述数目重估，设z是第一个用基于Aloha的方法估算出来的标签规模，x是已经被识别出的标签值，s是已经访问过的标签ID空间大小；自然，z-x就是待识别的标签数；根据剩余ID空间的节点密度，TH算法推到出总的标签数目是[(z-x)/(2b-s)]×2b，并使用它找到下一跳的节点；如果标签是均匀分布的，那么[(z-x)/(2b-s)]×2b＝z；

所述寻找跳频目的地，在最优层次重新计算完后，TH算法跳转到最大子树的根节点，这颗子树包含了待识别的标签且排除了之前已经识别过的标签，根节点所在的层数不能比新的最优层次小。

3.一种如权利要求1所述基于访问模式保护的空间数据安全控制系统的存储器可配置节能调度方法，其特征在于，该可配置节能调度的方法包括对多核嵌入式系统cache高速缓冲存储器应用性能监控器参数进行设置、多核嵌入式系统高速缓冲存储器的优化配置研究方法进行算法优化改进、通过对不同的高速缓冲存储器配置情况下性能指标的变化进行仿真、实现最合理优化的性能匹配；

高速缓冲存储器应用性能监控器参数进行设置是指利用计算机编制程序对多核嵌入式系统cache高速缓冲存储器的应用性能监控器参数进行反复设置，得到最佳的优化参数；

高速缓冲存储器的优化配置研究方法进行算法优化改进是指输入优化的监控器参数设置多核嵌入式系统高速缓冲存储器的优化配置方法，利用计算机程序对方法进行算法优化改进，得到最优的配置方法；

通过对不同的高速缓冲存储器配置情况下性能指标的变化进行仿真是指利用最优的配置方法分别通过对不同的高速缓冲存储器配置情况下的指标的变化进行仿真实验，得到不同的实验数据，选择最佳的实验结果；

实现最合理优化的性能匹配是指通过前面仿真实验结果，选定实验结果中能耗消耗尽可能小的配置进行实际项目的搭建，从而实现最合理优化的性能匹配。

4.如权利要求3所述的存储器可配置节能调度方法，其特征在于，进行算法优化改进步骤包括基于性能和公平性为基准的cache死亡块预测、cache访问失效、cache预取、基于性能和公平性为基准共享cache划分、能耗仿真计算；

基于性能和公平性为基准的cache死亡块预测是指首先通过对基于性能和公平性为基准的cache死亡块进行数据上的预测，为访问cache做好准备；

cache访问失效是指在访问cache过程时，会出现cache访问失效的结果；

cache预取是指在cache访问失效后，采取cache预取的措施；

基于性能和公平性为基准共享cache划分是指cache预取后，通过基于性能和公平性为

基准，共享cache的划分；

能耗仿真计算是指利用对cache的划分，设置能耗仿真模型进行能耗仿真计算，得到最优的计算结果。

5.如权利要求3所述的存储器可配置节能调度方法，其特征在于，存储器的优化配置研究方法进行算法优化改进中基于性能和公平性为基准共享cache划分步骤包括：

步骤一，进行线程基于性能的公平度变量计算；

步骤二，根据cache相关性原理，对可系统可分配cache块大小进行确定；

步骤三，对线程进行优先级的确认；

步骤四，根据线程优先级对线程进行cache块数量的分配；

步骤五，根据线程已分配的cache数量进行失效率公平性度量计算；

步骤六，从已经计算好的线程cache失效率公平性度量比较，如果线程个数大于二，则从中选出最大值和最小值线程；

步骤七，根据选出来的cache失效率公平性度量最大值与最小值的差值是否小于公平性度量变量临界值判定；如果为假，则对已分配两个线程的cache数量进行重新分配，重复进行步骤五和七；

步骤八，如果为真，则把这两个线程删掉，重复进行步骤六和七；

步骤九，如果线程数量为一个或者为零，算法结束。

6.一种如权利要求1所述基于访问模保护的空间数据安全控制系统的处理器非高斯噪声下数字调制信号识别方法，其特征在于，该识别方法包括：

步骤一，对接收信号s(t)进行非线性变换；对接收信号s(t)进行非线性变换，按如下公式进行：

$$f[s(t)]=\frac{s(t)*\ln|s(t)|}{|s(t)|}=s(t)c(t)$$

其中 $s(t)=\sum_{m=1}^{M}Aa(m)p(t-mT_b)\exp(j2\pi f_c t+\varphi(m))$ ，A表示信号的幅度，a(m)表示信号的码元符号，p(t)表示成形函数，f_c表示信号的载波频率，$\varphi(m)$表示信号的相位，通过该非线性变换后可得到：

$$f[s(t)]=s(t)\frac{ln|Aa(m)|}{|Aa(m)|}\ ;$$

步骤二，计算接收信号s(t)的广义一阶循环累积量$GC_{s,10}^{\beta}$和广义二阶循环累积量$GC_{s,21}^{\beta}$，通过计算接收信号s(t)的特征参数$M^1=\left|\left(GC_{s,10}^{\beta}\right)^2/GC_{s,21}^{\beta}\right|$和利用最小均方误差分类器，识别出2FSK信号；计算接受信号的广义循环累积量$GC_{s,10}^{\beta}$，按如下公式进行：

$$GC_{s,10}^{\beta}=GM_{s,10}^{\beta}\ ;$$

$$GC_{s,21}^{\beta}=GM_{s,21}^{\beta}\ ;$$

$GM_{s,10}^{\beta}$与$GM_{s,21}^{\beta}$均为广义循环矩，定义为：

$GM_{s,nm}^{\beta}=\left\langle f^{*}[s(t)]\cdots f^{*}[s(t)]f[s(t)]\cdots f[s(t)]\exp(-j2\pi\beta t)\right\rangle_{t}$，其中s(t)为信号，n为广义循环矩的阶数，共轭项为m项；

接收信号s(t)的特征参数M^1的理论值$M_{theory}^{1}=\left|\left(GC_{s,10}^{\beta}\right)^{2}/GC_{s,21}^{\beta}\right|$，具体计算过程如下进行：

$$GC_{s,10}^{\beta}=\frac{1}{N}\sum_{k=1}^{N}a(k)\left|\ln|a(k)|\right|$$

$$GC_{s,21}^{\beta}=\frac{1}{N}\sum_{k=1}^{N}a(k)a^{*}(k)\left|\ln|a(k)|\right|^{2}$$

经计算可知，对于2FSK信号，该信号的M_{theory}^{1}为1，而对于MSK、BPSK，QPSK、8PSK、16QAM和64QAM信号的M_{theory}^{1}均为0，由此可以通过最小均方误差分类器将2FSK信号识别出来，该分类器的表达形式为：

$$E_{1}=\min\left(M_{theory}^{1}-M_{actual}^{1}\right)^{2}\ ;$$

式中M_{actual}^{1}为特征参数M^1的实际值；

步骤三，计算接收信号s(t)的广义二阶循环累积量$GC_{s,20}^{\beta}$，通过计算接收信号s(t)的特征参数$M^{2}=\left|GC_{s,20}^{\beta}/GC_{s,21}^{\beta}\right|$和利用最小均方误差分类器，并通过检测广义循环累积量幅度谱β-$\left|GC_{s,20}^{\beta}\right|$的谱峰个数识别出BPSK信号和MSK信号；计算接收信号s(t)的广义二阶循环累积量$GC_{s,20}^{\beta}$，按如下公式进行：

$$GC_{s,20}^{\beta}=GM_{s,20}^{\beta}\ ;$$

接收信号s(t)的特征参数M^2的理论值$M_{theory}^{2}=\left|GC_{s,20}^{\beta}/GC_{s,21}^{\beta}\right|$，具体计算公式为：

$$GC_{s,20}^{\beta}=\frac{1}{N}\sum_{k=1}^{N}a(k)a(k)\left|\ln|a(k)|\right|^{2}$$

经过计算可知，BPSK信号和MSK信号的M_{theory}^{2}均为1，QPSK、8PSK、16QAM和64QAM信号的M_{theory}^{2}均为0，由此可以用最小均方误差分类器将BPSK、MSK信号与QPSK、8PSK、16QAM、64QAM信号分开；对于BPSK信号而言，在广义循环累积量幅度谱β-$\left|GC_{s,20}^{\beta}\right|$上仅在载频位置存在一个明显谱峰，而MSK信号在两个频率处各有一个明显谱峰，由此可通过特征参数M^2和检测广义循环累积量幅度谱β-$\left|GC_{s,20}^{\beta}\right|$的谱峰个数将BPSK信号与MSK信号识别出来；

检测广义循环累积量幅度谱β-$\left|GC_{s,20}^{\beta}\right|$的谱峰个数的具体方法如下：

首先搜索广义循环累积量幅度谱β-$\left|GC_{s,20}^{\beta}\right|$的最大值Max及其位置对应的循环频率$\alpha_0$，将其小邻域$[\alpha_0-\delta_0,\alpha_0+\delta_0]$内置零，其中$\delta_0$为一个正数，若$|\alpha_0-f_c|/f_c<\sigma_0$，其中$\delta_0$为一个接近0的正数，$f_c$为信号的载波频率，则判断此信号类型为BPSK信号，否则继续搜索次大值Max1及其位置对应的循环频率α_1；若$|Max-Max1|/Max<\sigma_0$，并且$|(\alpha_0+\alpha_1)/2-f_c|/f_c<\sigma_0$，则判断此信号类型为MSK信号；

步骤四，计算接收信号s(t)的广义四阶循环累积量$GC_{s,40}^{\beta}$，通过计算接收信号s(t)的特征参数$M^3=\left|GC_{s,40}^{\beta}/\left(GC_{s,21}^{\beta}\right)^2\right|$和利用最小均方误差分类器，识别出QPSK信号、8PSK信号、16QAM信号和64QAM信号；计算接收信号s(t)的广义二阶循环累积量$GC_{s,40}^{\beta}$，按如下公式进行：

$$GC_{s,40}^{\beta}=GM_{s,40}^{\beta}-3\left(GM_{s,20}^{\beta/2}\right)^2 ;$$

接收信号s(t)的特征参数M^3的理论值$M_{theory}^3=\left|GC_{s,40}^{\beta}/\left(GC_{s,21}^{\beta}\right)^2\right|$，具体计算过程如下

$$GC_{s,40}^{\beta}=\frac{1}{N}\sum_{k=1}^{N}[a(k)]^4\left|\ln|a(k)|\right|^4-3\left[\frac{1}{N}\sum_{k=1}^{N}[a(k)]^2\left|\ln|a(k)|\right|^2\right]^2$$

经过计算可知，QPSK信号的M_{theory}^3为1，8PSK信号的M_{theory}^3为0，16QAM信号的M_{theory}^3为0.5747，64QAM信号的M_{theory}^3为0.3580，由此通过最小均方误差分类器将QPSK、8PSK、16QAM和64QAM信号识别出来。

一种基于访问模式保护的空间数据安全控制系统

技术领域

[0001] 本发明属于电子信息安全控制系统技术领域，尤其涉及一种基于访问模式保护的空间数据安全控制系统。

背景技术

[0002] 随着计算机技术、网络技术的快速发展和应用普及，地域分散的多个组织实现了通过计算机网络进行远程动态交互和协同工作，基于网络的电子商务、电子政务、网络科研等活动逐步成为主流的应用模式。基于网络的跨域多组织大规模信息系统应用具有开放性、分布性、动态性的特征，因此跨域的访问控制呈现出资源的分布性、活动的动态性、主体的不可认知性等特征。如何在跨域访问控制中对服务提供者的资源进行有效控制同时保护服务请求者的隐私成为信息安全领域重要的研究热点之一。

[0003] 在分布式访问控制模型中，服务请求者通常将大量属性等信息披露给服务提供者，以便服务提供者根据属性信息依据控制策略赋予服务请求者权限。但是大量属性信息的披露容易造成隐私泄露，这给服务请求者带来了隐患和风险。因此，研究跨安全域访问控制方法，从而在多域互操作环境中保护服务请求者的隐私信息具有重大意义。

[0004] 目前，基于属性的访问控制模型使用访问控制UCON(Usage Control)是访问控制领域重要研究方向，UCON对传统的存取控制进行了扩展，定义了授权、义务和条件三个决定性因素，同时提出了访问控制的连续性和可变性两个重要属性。在传统的访问控制中，授权决策是在访问操作执行之前进行判断的，而在现代访问控制中，有相对长期持续的资源使用或立即撤消资源使用权限的应用要求，这些都需要在整个资源的使用过程中对访问请求进行实时监控，这一特征称为“连续性”。此外，在传统的访问控制中，属性只能通过管理行为才能被修改，然而在许多应用中，这些属性不得不因为主体的行为而被修改，对于可变属性的更新可能发生在使用资源之前，可能发生在使用的过程中，也可能发生在资源使用完成之后，这一特征称为“可变性”。连续性控制和可变属性使得基于历史的授权决策更容易实施。

[0005] 评价访问控制模型的安全性包括三个方面：保密性、完整性和可用性。其中，保密性指保证信息不泄露给未经授权的人；完整性指防止对信息的随意生成、修改和删除，保证信息从真实的信源无失真地传递到真实的信宿且不可重复；可用性保证信息系统应随时为授权使用者提供服务，防止由于病毒、黑客攻击造成的拒绝服务和被敌人利用。为了解决分布式访问控制模型中主体验证客体身份、通信通道安全可靠、客体验证主体提供的资源完整真实等安全问题，在设计系统时要采用一系列访问控制策略，实现安全的访问控制。现有的分布式访问控制机制中，服务请求者将大量属性披露给资源拥有者以此获得访问权限，这些属性通常包含了大量的隐私信息，在跨域安全访问控制环境中，无法对服务请求者进行有效的隐私保护。

[0006] RFID目前是物理访问控制系统中的主导技术。典型的这种系统是“卡”读取器，其通常安装在临近物理接入点(例如，在靠近门或者大门的墙上、或者在门或者大门上)。该读

取器读取在卡、钥匙扣大小存储器、贴纸或者类似形式要素中嵌入的RFID标签。最流行的RFID标签利用读/写存储器，并且许多卡读取器也能从标签存储器读取或者向标签存储器写入。

[0007] 目前四个标准在RFID通信中占主导地位：ISO/IEC14443-A、ISO/IEC14443-B、ISO/IEC15963、ISO/IEC18902和JIS X6319-4，据此通过引用将它们的每一个全部并入本文。过去十年间安装的大多数访问控制系统支持这些标准的一个或者多个，或者能升级来支持这些标准的一个或者多个。因此，在全球基础上遗留有大量使用这些标准的被安装的访问控制读取器。

[0008] 同样的RFID标准被用于其它应用，例如运输、行李识别、票务、根据非接触EMV标准(欧陆卡、万事达卡、维萨)的支付、以及更多应用。

[0009] 由于这些RFID标准的普遍实现，为了在例如智能电话和平板装置的移动装置中使用而开发的NFC技术在同样的RFID标准上建立起来。有人可能说NFC是嵌入在电话中的RFID，而不是嵌入在卡、钥匙扣大小存储器、标签或者甚至嵌入在电话中的卡读取器中的RFID。

[0010] NFC硬件可以是移动装置或电话的主要部分、或者可以是可移除的(例如，可移除NFC芯片或装置)。NFC装置可典型地在三种模式中的任何一种下操作，其中前两种模式使用最为普遍：(1)卡仿真模式；(2)读/写模式；以及(3)对等模式。

[0011] 在卡仿真模式中，NFC装置根据上述ISO标准仿真非接触卡，所述标准中的每一个据此通过引用全部并入本文。卡仿真模式的典型应用包括访问控制应用、以及支付和票务。

[0012] 在读/写模式中，该NFC装置读取标签，并且典型地基于从读取的标签获得的信息执行某项功能。该读/写模式的典型应用包括读取其附近带有NFC标签的海报、交互广告、发起移动网络(例如，自动网络浏览器激活)、自动短消息服务(SMS)、和自动呼叫开始。

[0013] 在对等模式中，允许两个NFC装置或者类似类型的装置彼此交换数据。对等模式的典型应用包括在两个装置之间设立无线设置(例如蓝牙、Wi-Fi等)、共享名片、或者共享信息。CN 103839313A说明书42/10页5卡仿真的意图是能够使用NFC装置作为在提到的应用(例如访问控制和支付)中的卡。

[0014] 该NFC卡仿真模式由移动网络运营商(MNO)经由在订户身份模块(SIM)卡或者一些其它已知装置(嵌入的或者可移除的)中的所谓安全元件来控制。如果用户的电话没有被天然装备有安全元件，那么用户可需要具有来自MNO的为NFC准备的新SIM卡。

[0015] 除了SIM卡之外，该NFC卡仿真应在电话的操作系统上使能。是否所有MNO包括这种选择以及用户如何获得这种选择是不清楚的，并且用户可能不得不预订和/或购买这个选择。因此，用于访问控制的NFC卡仿真将取决于：(1)MNO在移动网络中滚出(roll out of)NFC卡仿真的定时；以及(2)预订服务的成本和用户愿意支付什么。

[0016] 为了能够在卡仿真模式上独立于MNO的控制来使用用于访问控制的NFC电话，需要不同的方式来实现NFC卡仿真，包括开发能在传统卡读取器的安装基础上工作的方式。

发明内容

[0017] 本发明的目的在于提供一种基于访问模式保护的空间数据安全控制系统，旨在解决使用者的隐私保护，减少信息披露程度，阻止敏感信息泄露，实现使用者的空间数据安全

控制的问题。

[0018] 本发明是这样实现的，一种基于访问模式保护的空间数据安全控制系统，包括授权服务器、服务提供者、服务请求者、射频识别(RFID)读取器和RFID标签；所述授权服务器分别与服务请求者和服务提供者进行数据交互，所述服务请求者和服务提供者进行数据交互；

[0019] 所述射频识别(RFID)读取器包括电子组件，该电子组件使该RFID读取器能够生成射频(RF)场，并与位于该RF场内的RFID装置交换数据；RFID标签信号连接所述RFID读取器，所述射频识别(RFID)读取器与授权服务器信号连接。

[0020] 进一步，所述授权服务器对服务请求者授权指派，对服务请求者和服务提供者提供双方的公私密钥分发，并将安全域访问控制过程和隐私保护机制进行融合；所述授权服务器包括密钥库、属性库和策略库。

[0021] 进一步，所述密钥库用于保存服务请求者的授权公钥和服务提供者的加密私钥；所述属性库存储服务提供者模块和服务请求者模块的属性信息；所述策略库用于存储系统的决策策略；密钥库、属性库、策略库均具备对保存信息进行增加、删除、查找、备份功能。

[0022] 进一步，所述服务提供者是按权限集合的规定接受主体访问的被动实体，所述服务提供者包括策略提取模块和加密模块；

[0023] 所述策略提取模块通过发送客体属性进行策略提取；所述加密模块负责完成信息的加密工作，包含对资源设定的访问控制策略。

[0024] 进一步，所述服务请求者是对服务提供者拥有使用权限的主动实体，包括授权申请模块和解密模块；

[0025] 所述授权申请模块通过发送主体属性进行权限申请；所述解密模块负责完成信息的解密工作。

[0026] 进一步，所述RFID标签包括天线和存储器，所述RFID标签被配置为具有通过近场通信(NFC)装置向其存储器写入的加密私钥，并且其中所述RFID标签进一步被配置为通过所述NFC装置向所述RFID读取器传递向其存储器写入的加密私钥。

[0027] 进一步，所述RFID读取器还包括外壳，并且其中所述RFID标签位于该外壳内，向所述RFID标签的存储器写入的加密私钥被存储其中达到预定数量的时候被删除。

[0028] 进一步，所述RFID读取还包括天线，所述RFID标签的天线中心相对于所述RFID读取器的天线中心偏移，所述RFID读取器进一步被配置为命令所述RFID标签的控制电路将所述RFID标签的天线从所述RFID标签的集成电路(IC)脱离达到预定数量的时间，所述RFID读取器经由所述RF场和服务接口中的至少一个向所述RFID标签提供电力。

[0029] 进一步，所述近场通信(NFC)装置，包括处理器，所述处理器包括NFC模块的存储器和NFC接口，所述NFC模块被配置为确定所述NFC装置位于射频标识(RFID)读取器所产生的射频(RF)场内，并且响应于确定所述NFC装置位于所述RFID读取器产生的所述RF场内，向也位于所述RF场内的所述RFID标签写入访问控制加密私钥，使得所述RFID标签能代表所述NFC装置向所述RFID读取器传递所述访问控制加密私钥。

[0030] 进一步，所述的NFC装置，还包括使所述NFC装置能够接收该访问控制加密私钥的网络接口，所述NFC模块进一步使所述NFC装置在向所述RFID标签传递所述访问控制密钥之后，能够从所述RFID标签读回信息，从所述RFID标签读回的信息经由所述网络接口传送到

中央系统。

[0031] 本发明的另一目的在于提供一种所述基于访问模式保护的空间数据安全控制系统的RFID读取器识别概率最优树型跳跃协议的方法，所述RFID读取器识别概率最优树型跳跃协议的方法包括以下步骤：数目估算、计算最优跳转层、数目重估、寻找跳频目的地；

[0032] 首先估计出标签规模，然后根据标签规模，计算最优的树遍历层数以便使预期查询数最小，直接跳跃到那一层的最左节点；

[0033] 然后在那个节点的子树的执行DFT；

[0034] 经过对子树的遍历，估算剩下的没有被识别的标签规模，重新计算新的最优层数，直接跳跃到最优节点，并在那个节点的子树上执行DFT，直到所有的节点被识别出结束；

[0035] 所述数目估算，TH算法首先使用基于帧时隙Aloha的方法快速估算标签数量规模；

[0036] 所述计算最优跳转层，确定最优层次即TH算法直接跳转到的层次 γ_{op}；

[0037] 所述数目重估，设z是第一个用基于Aloha的方法估算出来的标签规模，x是已经被识别出的标签值，s是已经访问过的标签ID空间大小。自然，z-x就是待识别的标签数；根据剩余ID空间的节点密度，TH算法推到出总的标签数目是[(z-x)/(2b-s)]×2b，并使用它找到下一跳的节点；如果标签是均匀分布的，那么[(z-x)/(2b-s)]×2b＝z；

[0038] 所述寻找跳频目的地，在最优层次重新计算完后，TH算法跳转到最大子树的根节点，这颗子树包含了待识别的标签且排除了之前已经识别过的标签，根节点所在的层数不能比新的最优层次小。

[0039] 本发明的另一目的在于提供一种所述基于访问模式保护的空间数据安全控制系统的存储器可配置节能调度方法，该可配置节能调度的方法包括对多核嵌入式系统cache高速缓冲存储器应用性能监控器参数进行设置、多核嵌入式系统高速缓冲存储器的优化配置研究方法进行算法优化改进、通过对不同的高速缓冲存储器配置情况下性能指标的变化进行仿真、实现最合理优化的性能匹配；

[0040] 高速缓冲存储器应用性能监控器参数进行设置是指利用计算机编制程序对多核嵌入式系统cache高速缓冲存储器的应用性能监控器参数进行反复设置，得到最佳的优化参数；

[0041] 高速缓冲存储器的优化配置研究方法进行算法优化改进是指输入优化的监控器参数设置多核嵌入式系统高速缓冲存储器的优化配置方法，利用计算机程序对方法进行算法优化改进，得到最优的配置方法；

[0042] 通过对不同的高速缓冲存储器配置情况下性能指标的变化进行仿真是指利用最优的配置方法分别通过对不同的高速缓冲存储器配置情况下的指标的变化进行仿真实验，得到不同的实验数据，选择最佳的实验结果；

[0043] 实现最合理优化的性能匹配是指通过前面仿真实验结果，选定实验结果中能耗消耗尽可能小的配置进行实际项目的搭建，从而实现最合理优化的性能匹配。

[0044] 进一步，进行算法优化改进步骤包括基于性能和公平性为基准的cache死亡块预测、cache访问失效、cache预取、基于性能和公平性为基准共享cache划分、能耗仿真计算；

[0045] 基于性能和公平性为基准的cache死亡块预测是指首先通过对基于性能和公平性为基准的cache死亡块进行数据上的预测，为访问cache做好准备；

[0046] cache访问失效是指在访问cache过程时，会出现cache访问失效的结果；

[0047] cache预取是指在cache访问失效后，采取cache预取的措施；

[0048] 基于性能和公平性为基准共享cache划分是指cache预取后，通过基于性能和公平性为基准，共享cache的划分；

[0049] 能耗仿真计算是指利用对cache的划分，设置能耗仿真模型进行能耗仿真计算，得到最优的计算结果。

[0050] 进一步，存储器的优化配置研究方法进行算法优化改进中基于性能和公平性为基准共享cache划分步骤包括：

[0051] 步骤一，进行线程基于性能的公平度变量计算；

[0052] 步骤二，根据cache相关性原理，对可系统可分配cache块大小进行确定；

[0053] 步骤三，对线程进行优先级的确认；

[0054] 步骤四，根据线程优先级对线程进行cache块数量的分配；

[0055] 步骤五，根据线程已分配的cache数量进行失效率公平性度量计算；

[0056] 步骤六，从已经计算好的线程cache失效率公平性度量比较，如果线程个数大于二，则从中选出最大值和最小值线程；

[0057] 步骤七，根据选出来的cache失效率公平性度量最大值与最小值的差值是否小于公平性度量变量临界值判定；如果为假，则对已分配两个线程的cache数量进行重新分配，重复进行步骤五和七；

[0058] 步骤八，如果为真，则把这两个线程删掉，重复进行步骤六和七；

[0059] 步骤九，如果线程数量为一个或者为零，算法结束。

[0060] 本发明的另一目的在于提供一种所述基于访问模式保护的空间数据安全控制系统的处理器非高斯噪声下数字调制信号识别方法，该识别方法包括：

[0061] 步骤一，对接收信号s(t)进行非线性变换；对接收信号s(t)进行非线性变换，按如下公式进行：

[0062] $$f[s(t)]=\frac{s(t)*\ln|s(t)|}{|s(t)|}=s(t)c(t)$$

[0063] 其中 $s(t)=\sum_{m=1}^{M}Aa(m)p(t-mT_b)\exp(j2\pi f_c t+\varphi(m)))$ ，A表示信号的幅度，a(m)表示信号的码元符号，p(t)表示成形函数，f_c表示信号的载波频率，$\varphi(m)$表示信号的相位，通过该非线性变换后可得到：

[0064] $$f[s(t)]=s(t)\frac{ln|Aa(m)|}{|Aa(m)|}$$ ；

[0065] 步骤二，计算接收信号s(t)的广义一阶循环累积量$GC_{s,10}^{\beta}$和广义二阶循环累积量$GC_{s,21}^{\beta}$，通过计算接收信号s(t)的特征参数$M^1=\left|\left(GC_{s,10}^{\beta}\right)^2/GC_{s,21}^{\beta}\right|$和利用最小均方误差分类器，识别出2FSK信号；计算接受信号的广义循环累积量$GC_{s,10}^{\beta}$，按如下公式进行：

[0066] $GC_{s,10}^{\beta}=GM_{s,10}^{\beta}$ ；

[0067] $GC_{s,21}^{\beta}=GM_{s,21}^{\beta}$ ；

[0068] $GM_{s,10}^{\beta}$与$GM_{s,21}^{\beta}$均为广义循环矩，定义为：

[0069] $GM_{s,nm}^{\beta}=\left\langle f^{*}[s(t)]\cdots f^{*}[s(t)]f[s(t)]\cdots f[s(t)]\exp(-j2\pi\beta t)\right\rangle_{t}$ ，其中s(t)为信号，n为广义循环矩的阶数，共轭项为m项；

[0070] 接收信号s(t)的特征参数M^{1}的理论值$M_{theory}^{1}=\left|\left(GC_{s,10}^{\beta}\right)^{2}/GC_{s,21}^{\beta}\right|$ ，具体计算过程如下进行：

[0071] $$GC_{s,10}^{\beta}=\frac{1}{N}\sum_{k=1}^{N}a(k)\left|\ln|a(k)|\right|$$

[0072] $$GC_{s,21}^{\beta}=\frac{1}{N}\sum_{k=1}^{N}a(k)a^{*}(k)\left|\ln|a(k)|\right|^{2}$$

[0073] 经计算可知，对于2FSK信号，该信号的M_{theory}^{1}为1，而对于MSK、BPSK，QPSK、8PSK、16QAM和64QAM信号的M_{theory}^{1}均为0，由此可以通过最小均方误差分类器将2FSK信号识别出来，该分类器的表达形式为：

[0074] $E_{1}=\min\left(M_{theory}^{1}-M_{actual}^{1}\right)^{2}$ ；

[0075] 式中M_{actual}^{1}为特征参数M^{1}的实际值；

[0076] 步骤三，计算接收信号s(t)的广义二阶循环累积量$GC_{s,20}^{\beta}$ ，通过计算接收信号s(t)的特征参数$M^{2}=\left|GC_{s,20}^{\beta}/GC_{s,21}^{\beta}\right|$ 和利用最小均方误差分类器，并通过检测广义循环累积量幅度谱β-$\left|GC_{s,20}^{\beta}\right|$的谱峰个数识别出BPSK信号和MSK信号；计算接收信号s(t)的广义二阶循环累积量$GC_{s,20}^{\beta}$ ，按如下公式进行：

[0077] $GC_{s,20}^{\beta}=GM_{s,20}^{\beta}$ ；

[0078] 接收信号s(t)的特征参数M^{2}的理论值$M_{theory}^{2}=\left|GC_{s,20}^{\beta}/GC_{s,21}^{\beta}\right|$ ，具体计算公式为：

[0079] $$GC_{s,20}^{\beta}=\frac{1}{N}\sum_{k=1}^{N}a(k)a(k)\left|\ln|a(k)|\right|^{2}$$

[0080] 经过计算可知，BPSK信号和MSK信号的M_{theory}^{2}均为1，QPSK、8PSK、16QAM和64QAM信号的M_{theory}^{2}均为0，由此可以用最小均方误差分类器将BPSK、MSK信号与QPSK、8PSK、16QAM、64QAM信号分开；对于BPSK信号而言，在广义循环累积量幅度谱β-$\left|GC_{s,20}^{\beta}\right|$上仅在载频位置

存在一个明显谱峰，而MSK信号在两个频率处各有一个明显谱峰，由此可通过特征参数M^2和检测广义循环累积量幅度谱β-$\left|GC_{s,20}^{\beta}\right|$的谱峰个数将BPSK信号与MSK信号识别出来；

[0081] 检测广义循环累积量幅度谱β-$\left|GC_{s,20}^{\beta}\right|$的谱峰个数的具体方法如下：

[0082] 首先搜索广义循环累积量幅度谱β-$\left|GC_{s,20}^{\beta}\right|$的最大值Max及其位置对应的循环频率$\alpha_0$，将其小邻域$[\alpha_0-\delta_0,\alpha_0+\delta_0]$内置零，其中$\delta_0$为一个正数，若$|\alpha_0-f_c|/f_c<\sigma_0$，其中$\delta_0$为一个接近0的正数，$f_c$为信号的载波频率，则判断此信号类型为BPSK信号，否则继续搜索次大值Max1及其位置对应的循环频率α_1；若$|Max-Max1|/Max<\sigma_0$，并且$|(\alpha_0+\alpha_1)/2-f_c|/f_c<\sigma_0$，则判断此信号类型为MSK信号；

[0083] 步骤四，计算接收信号s(t)的广义四阶循环累积量$GC_{s,40}^{\beta}$，通过计算接收信号s(t)的特征参数$M^3=\left|GC_{s,40}^{\beta}/\left(GC_{s,21}^{\beta}\right)^2\right|$和利用最小均方误差分类器，识别出QPSK信号、8PSK信号、16QAM信号和64QAM信号；计算接收信号s(t)的广义二阶循环累积量$GC_{s,40}^{\beta}$，按如下公式进行：

[0084] $$GC_{s,40}^{\beta}=GM_{s,40}^{\beta}-3\left(GM_{s,20}^{\beta/2}\right)^2 ;$$

[0085] 接收信号s(t)的特征参数M^3的理论值$M_{theory}^3=\left|GC_{s,40}^{\beta}/\left(GC_{s,21}^{\beta}\right)^2\right|$，具体计算过程如下：

[0086] $$GC_{s,40}^{\beta}=\frac{1}{N}\sum_{k=1}^{N}[a(k)]^4\left|\ln|a(k)|\right|^4-3\left[\frac{1}{N}\sum_{k=1}^{N}[a(k)]^2\left|\ln|a(k)|\right|^2\right]^2$$

[0087] 经过计算可知，QPSK信号的M_{theory}^3为1，8PSK信号的M_{theory}^3为0，16QAM信号的M_{theory}^3为0.5747，64QAM信号的M_{theory}^3为0.3580，由此通过最小均方误差分类器将QPSK、8PSK、16QAM和64QAM信号识别出来。

[0088] 本发明提供的授权服务器模块包括了密钥库、属性库、策略库三部分。密钥库保存了服务请求者的授权公钥和服务提供者的加密私钥。属性库存储系统各方的属性信息。策略库存储系统的决策策略。密钥库、属性库、策略库均具备对保存信息进行增加、删除、查找、备份等基本功能，有效满足了访问控制过程中对信息源的要求。

[0089] 服务提供者模块中包括了策略提取模块和加密模块。策略提取模块通过发送客体属性进行策略提取。加密模块负责完成信息的加密工作，包含了对资源设定的访问控制策略。服务提供者的加密处理操作将策略隐含在加密密钥中，蕴含了对资源设定的访问控制规则，同时数据安全也得到了有效的保护。

[0090] 服务提请求者模块中包括了授权申请模块和解密模块。授权申请模块通过发送主体属性进行权限申请。解密模块负责完成信息的解密工作，等价于访问控制中的一致性验证过程。服务请求者的解密处理过程将个体的授权指派隐含在解密密钥中，蕴含了访问控制策略和用户所拥有的属性的一致性校验，解密操作完成了访问控制的一致性验证。将授权凭证跟解密密钥分量映射起来，并用策略表达式构造加密密钥分量，当且仅当请求者拥

有的加密密钥对应的解密密钥才能够解密，达到了在满足请求者在取得合法访问权限的同时使服务提供者尽可能少的获得请求者信息的安全目标。本发明在系统初始化、授权指派、策略定制、加密处理、消息恢复及验证过程中，完成跨安全域访问控制和隐私保护机制的融合，实现了对请求者隐私信息的保护，解决了跨安全域访问控制中服务请求者隐私泄露问题。

[0091] 有效加密私钥可对应于在RFID装置(例如，能够进行NFC的装置、RFID标签、不同的RFID标签等)和RFID读取器之间交换的数据结构。如访问控制领域已知的，可按照任何数目变型来提供访问控制加密私钥；然而，为了讨论容易，在RFID读取器和NFC装置之间交换的加密私钥可对应于能够被存储在计算机存储器中并经由RFID/NFC协议交换的任何数据结构(例如，加密、非加密等)。因此，可使用一个或多个NDEF记录或消息在NFC装置和RFID读取器之间交换加密私钥，并且密钥可对应于比特集合。除了需要有效加密私钥之外，RFID读取器可被装配为需要额外输入(例如密码、PIN、指纹等)，来证明NFC装置的持有者也知道某事、或者是具有开门的权限的某人。这种认证方法已知是双重因素认证方法。本发明把标签识别表示成为一个优化问题，并找到最优解从而确保最小的平均查询次数；有了坚实的理论基础，当标签规模从100变化到100K时，对于每个标签的总查询数，每个标签的总识别时间和每个标签的平均响应次数这3个指标，TH算法显著优于之前最优的标签识别算法达50％，10％和30％，其中标签ID是均匀分布的，当标签非均匀分布时，指标分别优于之前标签的26％，37％和26％。本发明提供的存储器可配置节能调度的方法，通过采用相应的高速缓冲存储器(Cache)优化配置，实现了对硬件性能最大限度的应用；通过对不同的高速缓冲存储器(Cache)配置进行仿真，以及多核嵌入式系统仿真基准集进行比较研究，寻找高速缓冲存储器(Cache)之间的相关性，进而从多核嵌入式系统在能量消耗和高速缓冲存储器(Cache)的单位面积利用率验证了所提出的研究方法正确性和有效性，最终实现了多核嵌入式系统数据管理能力、功耗的整体性能上的提高。本发明提供的非高斯噪声下数字调制信号的识别方法，对接收信号s(t)进行非线性变换；计算接收信号s(t)的广义一阶循环累积量$GC_{s,10}^{\beta}$和广义二阶循环累积量$GC_{s,21}^{\beta}$，通过计算接收信号s(t)的特征参数$M^1=\left|\left(GC_{s,10}^{\beta}\right)^2/GC_{s,21}^{\beta}\right|$和利用最小均方误差分类器，识别出2FSK信号；计算接收信号s(t)的广义二阶循环累积量$GC_{s,20}^{\beta}$，通过计算接收信号s(t)的特征参数$M^2=\left|GC_{s,20}^{\beta}/GC_{s,21}^{\beta}\right|$和利用最小均方误差分类器，并通过检测广义循环累积量幅度谱β-$\left|GC_{s,20}^{\beta}\right|$的谱峰个数识别出BPSK信号和MSK信号；计算接收信号s(t)的广义四阶循环累积量$GC_{s,40}^{\beta}$，通过计算接收信号s(t)的特征参数$M^3=\left|GC_{s,40}^{\beta}/\left(GC_{s,21}^{\beta}\right)^2\right|$和利用最小均方误差分类器，识别出QPSK信号、8PSK信号、16QAM信号和64QAM信号；本发明利用信号的广义循环累积量的三个特征参数，将信号集{2FSK、BPSK、MSK、QPSK、8PSK、16QAM、64QAM}中的信号识别出来，既解决了Alpha稳定分布噪声下的信号不具有二阶或二阶以上的统计量的问题，又提高了有效识别数字调制信号的性能，可用于对Alpha稳定分布噪声下的数字调制信号的调制方式类型进行识别，实用性强，具有较强的推广与应用价值。

附图说明

[0092] 图1是本发明实施例提供的基于访问模式保护的空间数据安全控制系统结构示意图。

[0093] 图2是本发明实施例提供的基于访问模式保护的空间数据安全控制系统控制方法流程图；

[0094] 图3是本发明实施例提供的基于访问模式保护的空间数据安全控制系统NFC装置示意图。

具体实施方式

[0095] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0096] 下面结合附图及具体实施例对本发明的应用原理作进一步描述。

[0097] 下面结合附图对本发明的应用原理作进一步描述。

[0098] 如图1：一种基于访问模式保护的空间数据安全控制系统，包括授权服务器、服务提供者、服务请求者、射频识别(RFID)读取器和RFID标签；所述授权服务器分别与服务请求者和服务提供者进行数据交互，所述服务请求者和服务提供者进行数据交互；

[0099] 所述射频识别(RFID)读取器包括电子组件，该电子组件使该RFID读取器能够生成射频(RF)场，并与位于该RF场内的RFID装置交换数据；RFID标签信号连接所述RFID读取器，所述射频识别(RFID)读取器与授权服务器信号连接。

[0100] 所述授权服务器对服务请求者授权指派，对服务请求者和服务提供者提供双方的公私密钥分发，并将安全域访问控制过程和隐私保护机制进行融合；所述授权服务器包括密钥库、属性库和策略库。

[0101] 所述密钥库用于保存服务请求者的授权公钥和服务提供者的加密私钥；所述属性库存储服务提供者模块和服务请求者模块的属性信息；所述策略库用于存储系统的决策策略；密钥库、属性库、策略库均具备对保存信息进行增加、删除、查找、备份功能。

[0102] 所述服务提供者是按权限集合的规定接受主体访问的被动实体，所述服务提供者包括策略提取模块和加密模块；

[0103] 所述策略提取模块通过发送客体属性进行策略提取；所述加密模块负责完成信息的加密工作，包含对资源设定的访问控制策略。

[0104] 所述服务请求者是对服务提供者拥有使用权限的主动实体，包括授权申请模块和解密模块；

[0105] 所述授权申请模块通过发送主体属性进行权限申请；所述解密模块负责完成信息的解密工作。

[0106] 所述RFID标签包括天线和存储器，所述RFID标签被配置为具有通过近场通信(NFC)装置向其存储器写入的加密私钥，并且其中所述RFID标签进一步被配置为通过所述NFC装置向所述RFID读取器传递向其存储器写入的加密私钥。

[0107] 所述RFID读取器还包括外壳，并且其中所述RFID标签位于该外壳内，向所述RFID

标签的存储器写入的加密私钥被存储其中达到预定数量的时候被删除。

[0108] 所述RFID读取还包括天线，所述RFID标签的天线中心相对于所述RFID读取器的天线中心偏移，所述RFID读取器进一步被配置为命令所述RFID标签的控制电路将所述RFID标签的天线从所述RFID标签的集成电路(IC)脱离达到预定数量的时间，所述RFID读取器经由所述RF场和服务接口中的至少一个向所述RFID标签提供电力。

[0109] 所述近场通信(NFC)装置，包括处理器，所述处理器包括NFC模块的存储器和NFC接口，所述NFC模块被配置为确定所述NFC装置位于射频标识(RFID)读取器所产生的射频(RF)场内，并且响应于确定所述NFC装置位于所述RFID读取器产生的所述RF场内，向也位于所述RF场内的所述RFID标签写入访问控制加密私钥，使得所述RFID标签能代表所述NFC装置向所述RFID读取器传递所述访问控制加密私钥。

[0110] 所述的NFC装置，还包括使所述NFC装置能够接收该访问控制加密私钥的网络接口，所述NFC模块进一步使所述NFC装置在向所述RFID标签传递所述访问控制密钥之后，能够从所述RFID标签读回信息，从所述RFID标签读回的信息经由所述网络接口传送到中央系统。

[0111] 下面结合具体实施例对本发明的应用原理作详细描述。

[0112] 授权服务器模块：授权服务器模块包括了密钥库、属性库、策略库三部分。密钥库保存了服务请求者的授权密钥和服务提供者的加密密钥。属性库存储属性信息。策略库存储系统的决策策略，策略库基于授权、义务和条件三个决策因素，并结合连续性和可变属性，设计出一套访问控制的策略模型。密钥库、属性库、策略库均具备对保存信息进行增加、删除、查找、备份等基本功能。

[0113] 服务提供者模块：服务提供者模块是按权限集合的规定接受主体访问的被动的实体(即客体)。客体可以是工作流系统中用到的信息、文件、记录等集合体，也可以是网络上的硬件设备，无线通信中的终端等。服务提供者模块中包括策略提取模块和加密模块。策略提取模块进行策略提取。加密模块负责完成信息的加密工作，包含了对资源设定的访问控制策略。

[0114] 服务请求者模块：服务请求者模块是可以对服务提供者拥有某些使用权限的一主动实体(即主体)。主体的含义很广泛，可以是用户所在的组织(用户组)、用户本身，也可以是用户使用的计算机终端、卡机、手持终端(无线)等，甚至可以是应用服务程序或进程。服务提请求者模块中包括了授权申请模块和解密模块。授权申请模块进行权限申请，其中，主体属性是访问决策过程使用的属性，标识了主体能力和特征，是权限决策过程中的重要参数，服务请求者需要通过授权申请模块定期或不定期向授权服务器更新自己的属性信息。解密模块负责完成信息的解密工作，等价于访问控制中的一致性验证过程。

[0115] 隐私保护算法：隐私保护算法在系统初始化、授权指派、策略定制、加密处理、消息恢复及验证过程中，完成跨安全域访问控制和隐私保护机制的融合。

[0116] 一种基于访问模式保护的空间数据安全控制系统控制方法：

[0117] (1)基于隐私保护的跨安全域访问控制系统初始化；

[0118] (2)服务请求者向授权服务器发送自己的标识ID请求授权凭证；

[0119] (3)授权服务器根据服务请求者标识ID分析服务请求者拥有的属性集；

[0120] (4)授权服务器计算授权解密密钥分量发送给服务请求者；

[0121] (5)服务提供者向授权服务器发送与本地策略相关的所有属性标识；

[0122] (6)授权服务器计算加密策略加密密钥分量发送给服务提供者；

[0123] (7)服务请求者向服务提供者发起服务请求；

[0124] (8)服务提供者计算服务请求者的授权解密密钥分量，并随机选取中间变量，令u＝H3(σ,m)；

[0125] (9)服务提供者根据请求资源标识提取策略表达式，并确定密文的元祖数；

[0126] (10)确定密文，并向服务请求者发送经过加密的资源响应信息；

[0127] (11)服务请求者从资源响应信息中提取策略表达式，同时确定密文的元祖数，并判断密文的第一个元祖数是否属于加法循环群；

[0128] (12)服务请求者根据策略表达式构造密钥，选取符合策略子项的属性组合；

[0129] (13)服务请求者重复计算，并验证U＝uP?

[0130] (14)服务请求者用解密密钥分量输出明文。

[0131] 其中，所述步骤(1)中，系统初始化由授权服务器完成，包括：给定安全参数k∈Z+，输入k产生大素数q，选择满足BDH问题难解的超奇异椭圆曲线E/GF(p)，通过E/GF(p)生成两个阶为q的群G1和G2，G1为加法循环群，G2为乘法循环群，双线性映射随机选取中间变量P∈G1；选取随机数。

[0132] 构造明文空间M＝{0,1}n。其中，所述步骤(2)中，标识ID的范围为ID∈{0,1}*；所述步骤(3)中，所述属性

[0133] 集用{a1,a2,...,am}表示。

[0134] 所述步骤(4)中，授权服务器通过计算将集合发送给服务请求者，集合即为授权服务器分发给服务请求者的授权解密密钥分量，在满足访问控制策略前提下(访问控制策略是资源拥有者制定，跟本算法没有太大关系，就是制定：具备什么样属性的用户可以访问具备什么样属性的资源，属于访问控制方法UCON的策略制定范畴)解密保密信息。

[0135] 所述步骤(5)中，所述属性标识用{a1,a2,...,an}表示。

[0136] 所述步骤(6)中，授权服务器通过计算将集合发送给服务提供者，集合即为授权服务器分发给服务提供者的授权加密密钥分量。

[0137] 所述步骤(7)中，所述服务请求用<ID,SID>表示，其中SID为资源标识。

[0138] 所述步骤(8)中，服务提供者计算服务请求者的授权解密密钥分量并随机选取中间变量σ∈(0,1)n，令u＝H3(σ,m)。

[0139] 所述步骤(9)中，服务提供者根据请求资源标识SID提取策略表达式{a i,1∧...∧a i,m}(这个表达式的每一个分量指的是属性，代表必须具备什么样的属性组合才能获得访问权限)，针对每个策略表达式分别确定密文的元祖数。针对每个资源有很多策略表达式，符合任何一个策略表达式都可以获得相应的权限，本表达式的每一个分量指的是针对每个策略表达式计算出来的相应的密文元祖分量，所有的策略表达式计算出的所有密文元祖共同组成密文。

[0140] 所述步骤(10)中，选取正整数确定密文(这个是位异或运算)，i＝1,...,k，向服务请求者发送经过加密的资源响应信息<Ploicy,C>；表示散列函数H3的散列空间；Ploicy是资源的访问策略。

[0141] 所述步骤(11)中，密文C的元祖数为k，令C＝<U,V1,...,Vk,W>，当密文的第一个元

祖数属于加法循环群，即则转入步骤(12)；当密文的第一个元祖数不属于加法循环群，即则拒绝密文。

[0142] 所述步骤(12)中，策略子项的属性组合解密密钥分量和加密密钥分量的系数均用{a1,a2,...,am}来表示，上限用n、m来表示，代表属性的个数，不会产生混乱，因为属性是统一划分的，有的属性用户和服务方都可以拥有的，属性集只是解密密钥分量和加密密钥分量的系数，表示加密分量，解密分量。

[0143] 所述步骤(13)中，服务请求者重复计算u＝H3(σ,m)，验证U＝uP，如果U＝uP，则验证成功，转入步骤(14)；否则拒绝密文；U表示加密密文C的第一个元组。

[0144] 所述步骤(2)-步骤(4)与步骤(5)-步骤(6)为并行关系。

[0145] 步骤(14)，否则拒绝密文；σ和m为计算的中间变量，u＝H3(σ,m)为映射，本算法中诸多加解密计算公式原理利用的是基于离散对数困难问题的加解密方法；

[0146] U表示加密密文C的第一个元组。加密时加密者利用公式U＝uP计算密文的第一个元祖数U然后发送密文，解密者利用私钥再次计算uP看是否与密文一致，如果一致表示密文能解密；判断的目的是利用双线性映射性质验证加解密的一致性。

[0147] 步骤(14)服务请求者用解密密钥分量输出明文。

[0148] 本发明运用隐私保护算法，在系统初始化、授权指派、策略定制、加密处理、消息恢复及验证过程中，完成跨安全域访问控制和隐私保护机制的融合，减少信息披露程度，阻止敏感信息泄露，实现服务请求者的隐私安全。

[0149] NFC装置120当呈现给RFID读取器时，可使得其中包括的NFC功能变得激活(例如由于RFID读取器产生的RF场导致的感应耦合)。一旦NFC装置靠近RFID读取器并已变得激活，则NFC装置进入读/写操作模式。当在这种操作模式中时，NFC装置向RFID标签写入其上存储的密钥或者密钥系列。

[0150] 一旦从NFC装置接收到密钥，标签就在其自身存储器中暂时存储这些密钥。随后，RFID读取器从RFID标签读取密钥，从而使得RFID读取器能从NFC装置获得密钥，而不需要NFC装置在卡仿真模式下操作。具体地，RFID装置能够经由RFID标签将密钥和其它数据传递到RFID读取器。

[0151] RFID标签可位于RFID读取器的面板后面。通过将RFID标签置于这个特殊的位置，RFID标签将保持靠近RFID读取器；因此，当将NFC装置呈现给RFID读取器时，NFC装置也置于RFID标签的通信范围内。

[0152] 应当理解的是，RFID标签不是必须置于RFID读取器的面板的后面；然而，这种位置为RFID标签提供方便的安装位置。但是，在其它实施例中，RFID标签可对应于位置靠近RFID读取器的贴纸等。

[0153] 相对于RFID读取器的天线的中心偏移RFID标签可为有利的。标签天线的中心如何相对于读取器天线的中心偏移。这种偏移对于最小化天线之间的寄生电容可能是有利的。读取器天线的中心可基本对准面板的中心。RFID读取器的电子组件可基本上置于读取器外壳的中心内。读取器天线可环绕外壳的外缘或者周界，因此读取器天线可在面板的中心附近居中。另一方面，由于RFID标签小于RFID读取器的电子组件，RFID标签可在读取器外壳内偏置。

[0154] 应该理解的是，RFID标签可使用任何类型的安全机制而保持在RFID读取器的外壳

内。作为一些非限制性示例，RFID标签可使用摩擦配件、胶水、粘合剂、双面胶、扣件(例如，螺母、螺钉(bolt)、螺杆(screw)等)、它们的任意组合、或者任何其它固定器装置，而保持在RFID读取器的外壳内。在一些实施例中，RFID标签可解除地安装在RFID读取器的外壳中，而在其它实施例中，RFID标签可永久固定在外壳中(例如，通过将RFID标签116的组件嵌入到外壳的塑料中)。

[0155] 将根据本公开实施例来描述RFID标签的组件。RFID标签可包括一个或者多个集成电路(ICs)、开关、控制电路、连接器和天线。在一些实施例中，RFID标签的组件可包括在已知的标签形式因素中，例如卡形式结构、钥匙扣大小存储器、贴纸等。尽管没描绘，但是RFID标签也可包括内部电源(例如，电池、太阳能电池和转换器等)，在该情况下RFID标签可被称为活动标签。另一方面，无源标签，不包括内部电源，取而代之的是，依赖于从与另一个RF场感应耦合的电力(例如，NFC装置120和/或RFID读取器112生成的场)。

[0156] IC404可对应于一个或者许多IC或者IC组件。具体地，IC404可包括当被外部RF场激活时生成并且传送预定响应的数字电路。在一些实施例中，IC404可包括除处理电路外的存储器。作为示例，IC404可包括足以存储访问控制密钥、加密密钥、加密算法、和它们的组合的存储器。

[0157] 在一些实施例中，IC404也为RFID标签提供安全功能。作为示例，IC404可为RFID标签提供加密算法，因此使RFID标签能够与其它装置(例如RFID读取器和NFC装置)交换加密通信。加密密钥等也可按照安全方式存储在IC404中。

[0158] 开关可为可选组件。在一些实施例中，IC104可被直接连接到天线，在该情况下RFID标签不需要开关和控制电路。在其它实施例中，开关可居于IC104和天线之间，并且由控制电路操作。作为示例，如上所述，天线可将噪声引入系统，在该系统中RFID读取器正尝试读取外部标签或者尝试从在仿真模式下操作的NFC装置直接读取密钥。如果这变成事实，则RFID读取器可配置为经由连接器提供指令到控制电路，以经由开关的动作从天线断开IC104。换句话说，如果RFID读取器确定RFID标签正引入太多噪声，那么RFID读取器可请求控制电路将开关从闭合位置移动到断开位置。

[0159] 开关可包括逻辑开关和/或物理开关。作为示例，开关可对应于在天线和IC104的连接器之间移动的物理开关。可替换地，开关可对应于软件开关、数字开关或者类似开关。

[0160] 控制电路可包括微控制器，其包括能够经由开关的动作对IC104和天线去耦合和去耦合的逻辑。控制电路从连接器接收其指令，连接器提供RFID标签和RFID读取器之间的接口。连接器可包括RFID标签和RFID读取器之间的有线端口或者无线接口(例如，第二天线)。

[0161] NFC装置可对应于移动通信装置，例如蜂窝电话、智能电话、平板电脑(tablet)、膝上电脑、或者任何其它使能NFC的装置。NFC装置被描述为包括处理器、存储器、NFC接口、和网络接口。在一些实施例中，处理器可对应于多个处理器，每个处理器被配置为执行NFC装置的某些操作。作为示例，NFC装置可具有用于其NFC功能和其它功能的专用处理器。在一些实施例中，NFC装置的组件可经由数据总线或者类似架构连接在一起。因此，尽管这些组件被描述为经由中央处理器连接，但是这种组件的排列是不需要的。

[0162] 处理器可对应于微处理器、中央处理单元(CPU)、处理器或者CPU的集合等。在一些实施例中，处理器可配置为执行存储在存储器中的指令，从而向NFC装置提供功能。

[0163] 存储器可包括多个模块或者其中存储的指令集(例如,应用、驱动等等)。在一些实施例中,存储器可包括易失性和/或非易失性存储器。作为一些非限制性的示例,存储器可包括NFC模块、浏览器、电话模块、电子邮件模块、和操作系统(O/S)536。NFC模块可包括指令,当其被处理器执行时,使能NFC装置的NFC功能。例如,NFC模块可负责促使NFC装置在卡仿真模式、读/写模式和/或对等模式下操作。NFC模块也可对应于存储器的特定部分,其中敏感数据(例如,(多个)密钥、加密算法、PIN(个人身份号码)、信用卡号、支付认证信息、其它交易数据等)被安全地存储在NFC装置上。作为示例,NFC模块可包括存储器的读/写保护区域,并且在一些情况下,该存储地点可被加密。应该注意的是,存储器可对应于除了NFC装置的安全元件之外的存储地点,安全元件传统上被实施为其中按照加密方式存储NFC数据的SIM卡或者嵌入式安全元件,因为这种形式的安全元件将可能被MNO(运营商)控制。因此,除了为处理器提供可执行指令之外,NFC模块可对应于特定存储器或者存储地点。

[0164] 当执行指令时,NFC模块可促使处理器根据已知的NFC协议经由NFC接口与其它装置交换信息。在一些实施例中,NFC接口可包括与其它使能RF的装置创建感应耦合的线圈或者天线。NFC接口的大小可取决于NFC装置和NFC装置中包含的其他天线的总大小。NFC装置其它的电话功能可通过存储器中存储的其它模块O/S536提供。作为示例,O/S536可对应于特别为智能电话等设计的移动操作系统。O/S536的非限制性示例包括安卓黑莓Windows和类似系统。O/S536除了协调存储器中存储的应用和其它模块的操作,可负责提供电话的基本功能(例如,控制用户输入和输出功能、麦克风功能、协调驱动器等)。

[0165] 浏览器可为NFC装置提供浏览例如因特网的能力。在一些实施例中,浏览器对应于这样的应用,该应用使NFC装置能够使用已知因特网协议(例如,HTTP、HTML、XML等)在通信网络上与服务器和其它数据提供商交换信息。浏览器的非限制性示例包括Internet Google它们的移动版本等。

[0166] 电话模块可为NFC装置提供启动和应答呼叫的能力(例如,语音呼叫、视频呼叫、多媒体协作等)。电话模块也可使用户能够执行高级的通信功能,例如访问语音邮件、建立会议呼叫等。

[0167] 电子邮件模块可为NFC装置提供在通信网络上与其它装置交换电子消息的能力。作为示例,电子邮件模块可特别支持电子邮件通信。还应该理解的是电子邮件模块可支持其它类型的通信,例如社交媒体通信(例如,等)、短消息服务(SMS)消息传送、多媒体消息传送服务(MMS)、通过因特网(例如,根据IP协议)传送的数据消息等。

[0168] NFC装置和更广泛的通信网络之间的通信可通过网络接口变得便利,网络接口实际可包括几个不同网络或者网络类型的接口。例如,网络接口可包括使NFC装置能够与通常由MNO提供的蜂窝网络交互的蜂窝网络接口。网络接口可替地或者附加地包括802.11N接口(例如,Wi-Fi接口)、通用串行总线(USB)端口、或者到NFC装置的通信总线的任何其它有线或者无线接口。

[0169] 本发明的另一目的在于提供一种所述基于访问模保护的空间数据安全控制系统的RFID读取器识别概率最优树型跳跃协议的方法,所述RFID读取器识别概率最优树型跳跃协议的方法包括以下步骤:数目估算、计算最优跳转层、数目重估、寻找跳频目的地;

[0170] 首先估计出标签规模,然后根据标签规模,计算最优的树遍历层数以便使预期查询数最小,直接跳跃到那一层的最左节点;

[0171] 然后在那个节点的子树的执行DFT；

[0172] 经过对子树的遍历，估算剩下的没有被识别的标签规模，重新计算新的最优层数，直接跳跃到最优节点，并在那个节点的子树上执行DFT，直到所有的节点被识别出结束；

[0173] 所述数目估算，TH算法首先使用基于帧时隙Aloha的方法快速估算标签数量规模；

[0174] 所述计算最优跳转层，确定最优层次即TH算法直接跳转到的层次γ_{op}；

[0175] 所述数目重估，设z是第一个用基于Aloha的方法估算出来的标签规模，x是已经被识别出的标签值，s是已经访问过的标签ID空间大小。自然，z-x就是待识别的标签数；根据剩余ID空间的节点密度，TH算法推到出总的标签数目是[(z-x)/(2b-s)]×2b，并使用它找到下一跳的节点；如果标签是均匀分布的，那么[(z-x)/(2b-s)]×2b＝z；

[0176] 所述寻找跳频目的地，在最优层次重新计算完后，TH算法跳转到最大子树的根节点，这颗子树包含了待识别的标签且排除了之前已经识别过的标签，根节点所在的层数不能比新的最优层次小。

[0177] 本发明的另一目的在于提供一种所述基于访问模式保护的空间数据安全控制系统的存储器可配置节能调度方法，该可配置节能调度的方法包括对多核嵌入式系统cache高速缓冲存储器应用性能监控器参数进行设置、多核嵌入式系统高速缓冲存储器的优化配置研究方法进行算法优化改进、通过对不同的高速缓冲存储器配置情况下性能指标的变化进行仿真、实现最合理优化的性能匹配；

[0178] 高速缓冲存储器应用性能监控器参数进行设置是指利用计算机编制程序对多核嵌入式系统cache高速缓冲存储器的应用性能监控器参数进行反复设置，得到最佳的优化参数；

[0179] 高速缓冲存储器的优化配置研究方法进行算法优化改进是指输入优化的监控器参数设置多核嵌入式系统高速缓冲存储器的优化配置方法，利用计算机程序对方法进行算法优化改进，得到最优的配置方法；

[0180] 通过对不同的高速缓冲存储器配置情况下性能指标的变化进行仿真是指利用最优的配置方法分别通过对不同的高速缓冲存储器配置情况下的指标的变化进行仿真实验，得到不同的实验数据，选择最佳的实验结果；

[0181] 实现最合理优化的性能匹配是指通过前面仿真实验结果，选定实验结果中能耗消耗尽可能小的配置进行实际项目的搭建，从而实现最合理优化的性能匹配。

[0182] 进一步，进行算法优化改进步骤包括基于性能和公平性为基准的cache死亡块预测、cache访问失效、cache预取、基于性能和公平性为基准共享cache划分、能耗仿真计算；

[0183] 基于性能和公平性为基准的cache死亡块预测是指首先通过对基于性能和公平性为基准的cache死亡块进行数据上的预测，为访问cache做好准备；

[0184] cache访问失效是指在访问cache过程时，会出现cache访问失效的结果；

[0185] cache预取是指在cache访问失效后，采取cache预取的措施；

[0186] 基于性能和公平性为基准共享cache划分是指cache预取后，通过基于性能和公平性为基准，共享cache的划分；

[0187] 能耗仿真计算是指利用对cache的划分，设置能耗仿真模型进行能耗仿真计算，得到最优的计算结果。

[0188] 进一步，存储器的优化配置研究方法进行算法优化改进中基于性能和公平性为基

准共享cache划分步骤包括：

[0189] 步骤一，进行线程基于性能的公平度变量计算；

[0190] 步骤二，根据cache相关性原理，对可系统可分配cache块大小进行确定；

[0191] 步骤三，对线程进行优先级的确认；

[0192] 步骤四，根据线程优先级对线程进行cache块数量的分配；

[0193] 步骤五，根据线程已分配的cache数量进行失效率公平性度量计算；

[0194] 步骤六，从已经计算好的线程cache失效率公平性度量比较，如果线程个数大于二，则从中选出最大值和最小值线程；

[0195] 步骤七，根据选出来的cache失效率公平性度量最大值与最小值的差值是否小于公平性度量变量临界值判定；如果为假，则对已分配两个线程的cache数量进行重新分配，重复进行步骤五和七；

[0196] 步骤八，如果为真，则把这两个线程删掉，重复进行步骤六和七；

[0197] 步骤九，如果线程数量为一个或者为零，算法结束。

[0198] 本发明的另一目的在于提供一种所述基于访问模保护的空间数据安全控制系统的处理器非高斯噪声下数字调制信号识别方法，该识别方法包括：

[0199] 步骤一，对接收信号s(t)进行非线性变换；对接收信号s(t)进行非线性变换，按如下公式进行：

[0200] $$f[s(t)]=\frac{s(t)*\ln|s(t)|}{|s(t)|}=s(t)c(t)$$

[0201] 其中$s(t)=\sum_{m=1}^{M}Aa(m)p(t-mT_b)\exp(j2\pi f_c t+\varphi(m)))$，A表示信号的幅度，a(m)表示信号的码元符号，p(t)表示成形函数，f_c表示信号的载波频率，$\varphi(m)$表示信号的相位，通过该非线性变换后可得到：

[0202] $$f[s(t)]=s(t)\frac{ln|Aa(m)|}{|Aa(m)|}$$；

[0203] 步骤二，计算接收信号s(t)的广义一阶循环累积量$GC_{s,10}^{\beta}$和广义二阶循环累积量$GC_{s,21}^{\beta}$，通过计算接收信号s(t)的特征参数$M^1=\left|\left(GC_{s,10}^{\beta}\right)^2/GC_{s,21}^{\beta}\right|$和利用最小均方误差分类器，识别出2FSK信号；计算接受信号的广义循环累积量$GC_{s,10}^{\beta}$，按如下公式进行：

[0204] $$GC_{s,10}^{\beta}=GM_{s,10}^{\beta}$$；

[0205] $$GC_{s,21}^{\beta}=GM_{s,21}^{\beta}$$；

[0206] $GM_{s,10}^{\beta}$与$GM_{s,21}^{\beta}$均为广义循环矩，定义为：

[0207] $$GM_{s,nm}^{\beta}=\left\langle f^*[s(t)]\cdots f^*[s(t)]f[s(t)]\cdots f[s(t)]\exp(-j2\pi\beta t)\right\rangle_t$$，其中s(t)为信号，n为

广义循环矩的阶数，共轭项为m项；

[0208] 接收信号s(t)的特征参数M^1的理论值$M^1_{theory}=\left|\left(GC^{\beta}_{s,10}\right)^2/GC^{\beta}_{s,21}\right|$，具体计算过程如下进行：

[0209] $$GC^{\beta}_{s,10}=\frac{1}{N}\sum_{k=1}^{N}a(k)\left|\ln|a(k)|\right|$$

[0210] $$GC^{\beta}_{s,21}=\frac{1}{N}\sum_{k=1}^{N}a(k)a^*(k)\left|\ln|a(k)|\right|^2$$

[0211] 经计算可知，对于2FSK信号，该信号的M^1_{theory}为1，而对于MSK、BPSK，QPSK、8PSK、16QAM和64QAM信号的M^1_{theory}均为0，由此可以通过最小均方误差分类器将2FSK信号识别出来，该分类器的表达形式为：

[0212] $$E_1=\min\left(M^1_{theory}-M^1_{actual}\right)^2$$；

[0213] 式中M^1_{actual}为特征参数M^1的实际值；

[0214] 步骤三，计算接收信号s(t)的广义二阶循环累积量$GC^{\beta}_{s,20}$，通过计算接收信号s(t)的特征参数$M^2=\left|GC^{\beta}_{s,20}/GC^{\beta}_{s,21}\right|$和利用最小均方误差分类器，并通过检测广义循环累积量幅度谱β-$\left|GC^{\beta}_{s,20}\right|$的谱峰个数识别出BPSK信号和MSK信号；计算接收信号s(t)的广义二阶循环累积量$GC^{\beta}_{s,20}$，按如下公式进行：

[0215] $$GC^{\beta}_{s,20}=GM^{\beta}_{s,20}$$；

[0216] 接收信号s(t)的特征参数M^2的理论值$M^2_{theory}=\left|GC^{\beta}_{s,20}/GC^{\beta}_{s,21}\right|$，具体计算公式为：

[0217] $$GC^{\beta}_{s,20}=\frac{1}{N}\sum_{k=1}^{N}a(k)a(k)\left|\ln|a(k)|\right|^2$$

[0218] 经过计算可知，BPSK信号和MSK信号的M^2_{theory}均为1，QPSK、8PSK、16QAM和64QAM信号的M^2_{theory}均为0，由此可以用最小均方误差分类器将BPSK、MSK信号与QPSK、8PSK、16QAM、64QAM信号分开；对于BPSK信号而言，在广义循环累积量幅度谱β-$\left|GC^{\beta}_{s,20}\right|$上仅在载频位置存在一个明显谱峰，而MSK信号在两个频率处各有一个明显谱峰，由此可通过特征参数M^2和检测广义循环累积量幅度谱β-$\left|GC^{\beta}_{s,20}\right|$的谱峰个数将BPSK信号与MSK信号识别出来；

[0219] 检测广义循环累积量幅度谱β-$\left|GC^{\beta}_{s,20}\right|$的谱峰个数的具体方法如下：

[0220] 首先搜索广义循环累积量幅度谱β-$\left|GC^{\beta}_{s,20}\right|$的最大值Max及其位置对应的循环频率$\alpha_0$，将其小邻域$[\alpha_0-\delta_0,\alpha_0+\delta_0]$内置零，其中$\delta_0$为一个正数，若$|\alpha_0-f_c|/f_c<\sigma_0$，其中$\delta_0$为一个

接近0的正数，f_c为信号的载波频率，则判断此信号类型为BPSK信号，否则继续搜索次大值Max1及其位置对应的循环频率α_1；若$|Max-Max1|/Max<\sigma_0$，并且$|(\alpha_0+\alpha_1)/2-f_c|/f_c<\sigma_0$，则判断此信号类型为MSK信号；

[0221] 步骤四，计算接收信号s(t)的广义四阶循环累积量$GC_{s,40}^{\beta}$，通过计算接收信号s(t)的特征参数$M^3=\left|GC_{s,40}^{\beta}/\left(GC_{s,21}^{\beta}\right)^2\right|$和利用最小均方误差分类器，识别出QPSK信号、8PSK信号、16QAM信号和64QAM信号；计算接收信号s(t)的广义二阶循环累积量$GC_{s,40}^{\beta}$，按如下公式进行：

[0222] $GC_{s,40}^{\beta}=GM_{s,40}^{\beta}-3\left(GM_{s,20}^{\beta/2}\right)^2$；

[0223] 接收信号s(t)的特征参数M^3的理论值$M_{theory}^3=\left|GC_{s,40}^{\beta}/\left(GC_{s,21}^{\beta}\right)^2\right|$，具体计算过程如下：

[0224] $$GC_{s,40}^{\beta}=\frac{1}{N}\sum_{k=1}^{N}[a(k)]^4\left|\ln|a(k)|\right|^4-3\left[\frac{1}{N}\sum_{k=1}^{N}[a(k)]^2\left|\ln|a(k)|\right|^2\right]^2$$

[0225] 经过计算可知，QPSK信号的M_{theory}^3为1，8PSK信号的M_{theory}^3为0，16QAM信号的M_{theory}^3为0.5747，64QAM信号的M_{theory}^3为0.3580，由此通过最小均方误差分类器将QPSK、8PSK、16QAM和64QAM信号识别出来。

[0226] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

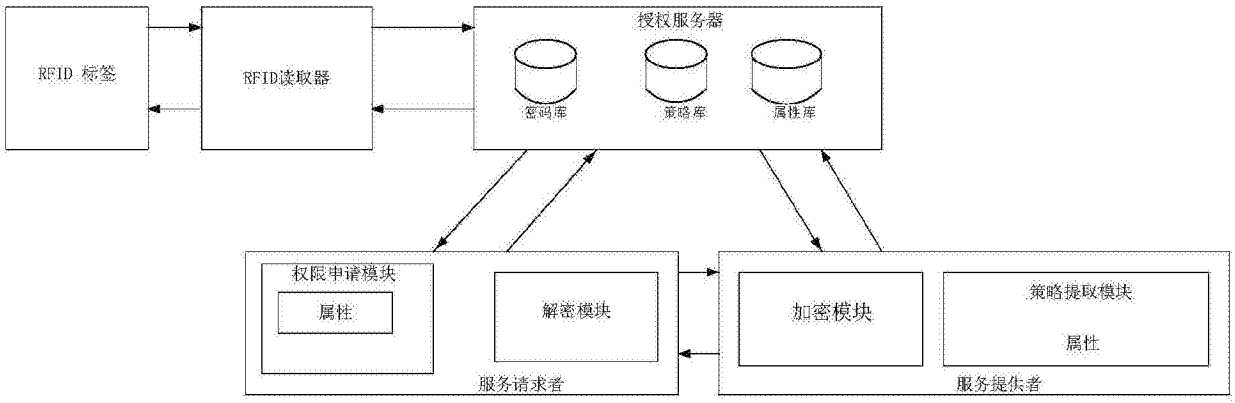

RFID 标签
RFID读取器
授权服务器
密码库
策略库
属性库
权限申请模块
属性
解密模块
服务请求者
加密模块
策略提取模块
属性
服务提供者

图1

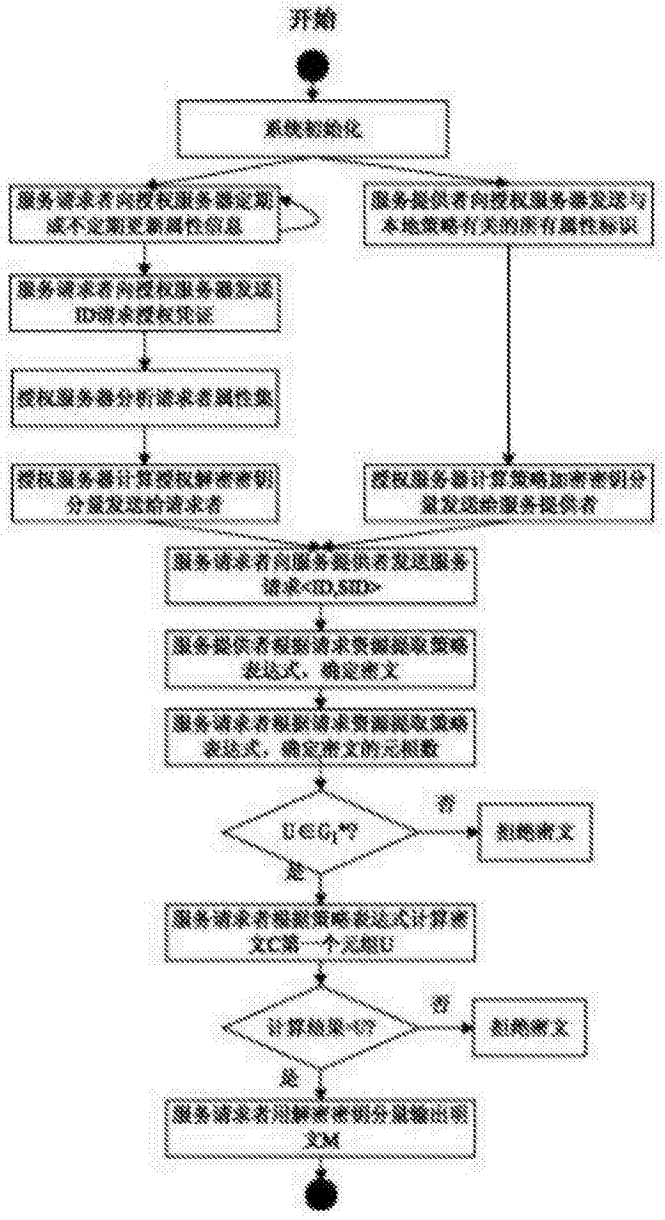

开始
系统初始化
服务请求者向授权服务器发送属
性集合
服务提供者向授权服务器发送与
本地策略有关的所有属性标识
服务请求者向授权服务器发送
ID请求授权凭证
授权服务器分析请求者属性集
授权服务器计算授权解密密钥
分量发送给请求者
授权服务器计算策略加密密钥分
量发送给服务提供者
服务请求者向服务提供者发送服务
请求<ID,SID>
服务提供者根据请求资源获取策略
表达式，确定密文
服务请求者根据请求资源获取策略
表达式，确定密文的元组数
否
丢弃密文
是
服务请求者根据策略表达式计算密
文C第一个元组U
否
丢弃密文
是
服务请求者用解密密钥分量输出明
文M

图2

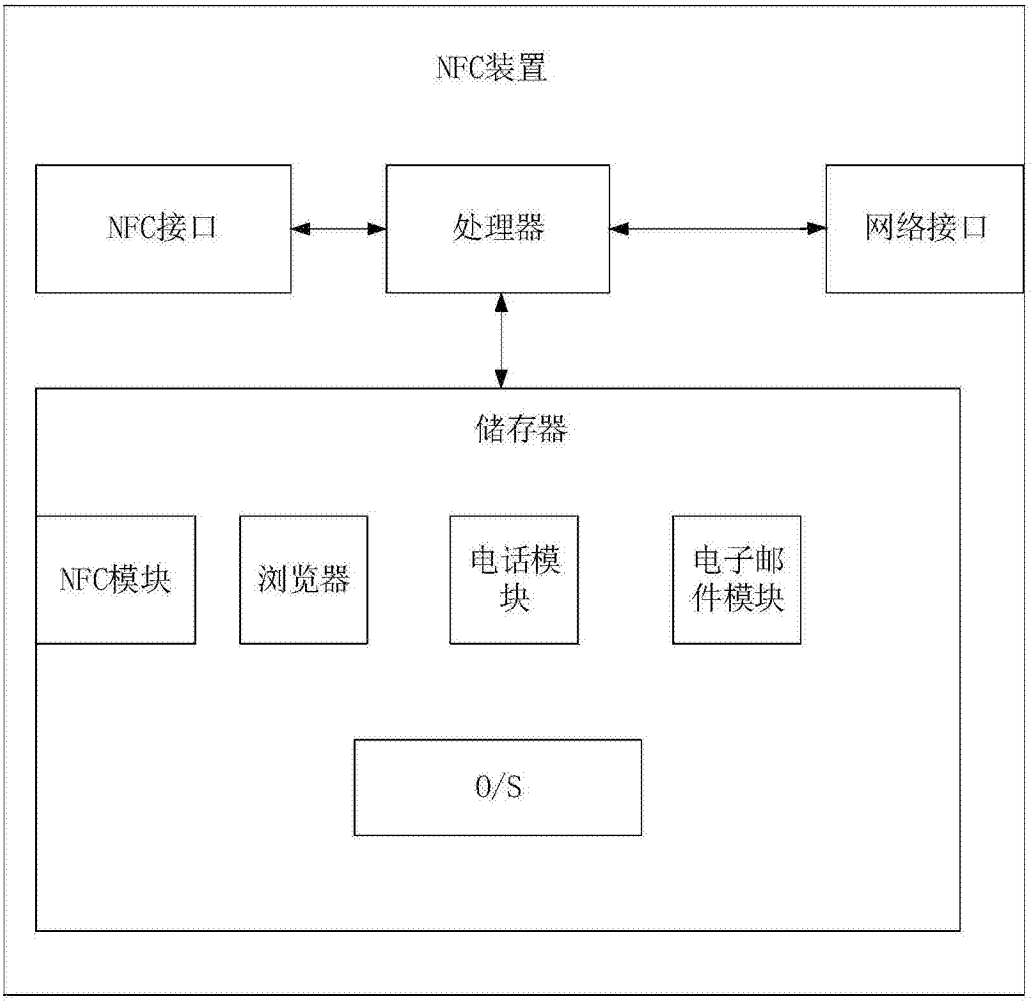


图3