(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102902932 B
(45)授权公告日 2015.12.02

(21)申请号 201210345952.8

(22)申请日 2012.09.18

(73)专利权人 武汉华工安鼎信息技术有限责任公司
地址 430223 湖北省武汉市高新开发区武大科技园路 7 号武大航域 C1 栋

(72)发明人 景奕昕 韩敏 余鹏飞 唐威 廖巍

(74)专利代理机构 湖北武汉永嘉专利代理有限公司 42102
代理人 王超

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 17/30(2006.01)

(56)对比文件
CN 101587479 A,2009.11.25, 说明书第 3 页第 1-17 段,附图 3-7.
CN 101587479 A,2009.11.25, 全文 .
郑向军 . 数据库加密系统的设计与实现 .《中国优秀硕士学位论文全文数据库》.2012,(第 02 期), 第 27-44 页 .
郑向军 . 数据库加密系统的设计与实现 .《中国优秀硕士学位论文全文数据库》.2012,(第 02 期), 第 27-44 页 .

审查员 张琳

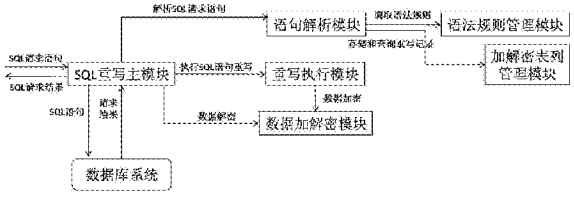
权利要求书1页 说明书6页 附图3页

(54)发明名称

基于 SQL 重写的数据库外部加解密系统的使用方法

(57)摘要

本发明提供了一种基于 SQL 重写的数据库加解密系统及其使用方法。该系统包括 SQL 重写主模块、语句解析模块、语法规则管理模块、加解密表列管理模块、重写执行模块以及数据加解密模块。该方法包括执行重写后的数据表的创建过程、重写后的数据的插入过程和数据的查询过程。本发明采用 SQL 重写技术,在数据库系统外部对数据进行加解密,从而避免数据库系统加解密开销。



CN 102902932 B

1. 基于 SQL 重写的数据库外部加解密系统的使用方法，其特征在于：包括执行重写后的数据表的创建过程、重写后的数据的插入过程和数据的查询过程；

所述数据表的创建过程包括：

A1) 创建含有加密列数据表的 SQL 语句通过 SQL 重写主模块进入语句解析模块；

A2) 语句解析模块调用语法规则管理模块获知需要加密的数据表列及其加密算法；

A3) 语句解析模块判断 SQL 语句是否合法，若否，过程终止，若合法，进入下一步；

A4) 语句解析模块生成 SQL 重写记录，该记录记载了加密的表列和相应的加密算法名称，以及加密后的数据类型；

A5) 重写记录由加解密表列管理模块进行存储；

A6) 语句解析模块将 SQL 重写记录返回给 SQL 重写主模块，SQL 重写主模块再将重写记录和待重写的 SQL 语句交由重写执行模块执行；

A7) 重写执行模块根据重写记录将含有加密列数据表的 SQL 语句重写成标准 SQL 语句，修改列数据类型为加密后的数据类型，然后将重写后的 SQL 请求语句送交 SQL 重写主模块；

A8) 重写后的 SQL 请求语句被送往数据库系统创建数据表；

所述数据的插入过程包括：

B1) SQL 重写主模块将执行数据插入的 SQL 语句输入语句解析模块；

B2) 语句解析模块根据加解密表列管理模块的记录，逐个检查每个数据列是否已记载在 SQL 重写记录中，若否，不做任何重写，执行 B6；若为是，则该数据列需要进行加密处理，进入下一步；

B3) 语句解析模块将需要加密的表列和相应的加密算法名发送给 SQL 重写主模块；

B4) SQL 重写主模块将包含需加密表列数据的 SQL 语句发送给重写执行模块，重写执行模块调用数据加解密模块进行加密，得到加密后的表列数据；

B5) 重写执行模块将 SQL 语句中的需加密的表列数据替换为加密后的表列数据，并返回给 SQL 重写主模块；

B6) SQL 重写主模块将数据插入语句送往数据库系统；

所述数据的查询过程包括：

C1) SQL 重写主模块接收从数据库系统查询数据的 SQL 请求语句，并发送给语句解析模块；

C2) 语句解析模块根据加解密表列管理模块的记录，逐个检查待查询的数据列是否记录在该记录中，若否，执行步骤 C5；若为是，则该数据列需要进行解密处理，进入下一步；

C3) 语句解析模块将需要解密的表列和相应的加密算法名发送给 SQL 重写主模块；

C4) SQL 重写主模块将需要解密的数据表列列为待处理项；

C5) SQL 重写主模块将 SQL 查询语句发往数据库得到查询结果；

C6) 对于查询结果，SQL 重写主模块检查是否包含有待处理项，若否，执行步骤 C8；若为是，进入下一步；

C7) SQL 重写主模块调用数据加解密模块中相应的加密算法，将待处理项进行解密；

C8) SQL 重写主模块返回最终的查询结果。

基于 SQL 重写的数据库外部加解密系统的使用方法

技术领域

[0001] 本发明涉及数据库加密领域，尤其涉及一种基于 SQL 重写技术的数据库加解密方法。

背景技术

[0002] 隐私数据的泄露是当前数据库系统面临的一个严重威胁。恶意的数据库管理员可通过访问数据库管理系统服务器去获取隐私数据（包括健康记录、金融股票、个人信息等）并出售给第三者。一种解决此威胁的方式是将数据库中的敏感数据进行加密，但多数数据库系统不适合使用这种方式。这种方式会产生很多无法克服的负面影响。首先，数据库系统要处理大量用户和程序的查询请求并生成数据返回，大量的保密数据和有效查询执行性能之间存在严重冲突。当前针对密文数据的计算方式或是效率低下或是不能提供充分的保密性，如使用强加密算法所得到密文数据会阻止数据库服务器执行 SQL 查询命令。其次，当前数据库加密系统在查询中必须先对加密数据表解密，然后用明文数据与查询 SQL 进行匹配，导致明文数据暴露在数据库系统中，数据库管理人员有机会盗取明文敏感数据。此外，数据库端对查询结果进行解密操作，查询结果以明文的方式返回给应用层，在传输过程中易遭窃取，导致敏感数据泄露。

[0003] 基于以上情况，必须采取高效、安全的加密手段，提升数据库加密的安全性和执行效率。

发明内容

[0004] 本发明目的在于提供一种基于 SQL 重写的数据库加解密方法，使用本发明能够集 SQL 重写、数据加密、数据解密、安全传输、高效查询于一体，实现对数据库加密数据创建和使用的安全防护。

[0005] 本发明所采用的技术方案是：基于 SQL 重写的数据库外部加解密系统，包括 SQL 重写主模块、语句解析模块、语法规则管理模块、加解密表列管理模块、重写执行模块以及数据加解密模块；

[0006] SQL 重写主模块在数据库查询过程中，根据加解密需求对语句解析模块、重写执行模块、数据加解密模块和加解密表列管理模块进行调度；

[0007] 语句解析模块负责对 SQL 语句进行语法和语义检查，生成 SQL 语句重写记录存储在加解密表列管理模块中；

[0008] 语法规则管理模块定义了和加解密相关的 SQL 语句关键字，供语句解析模块参考；

[0009] 加解密表列管理模块对数据库中已加密的表列和加解密算法进行记录；

[0010] 重写执行模块受 SQL 重写主模块调用，执行 SQL 语句的重写，并与数据加解密模块进行数据通信；

[0011] 数据加解密模块负责对输入值按照给定的加解密算法进行加密或者解密。

[0012] 基于 SQL 重写的数据库外部加解密系统的使用方法，包括执行重写后的数据表的创建过程、重写后的数据的插入过程和数据的查询过程。

[0013] 所述的使用方法，数据表的创建过程包括：

[0014] A1) 创建含有加密列数据表的 SQL 语句通过 SQL 重写主模块进入语句解析模块；

[0015] A2) 语句解析模块调用语法规则管理模块获知需要加密的数据表列及其加密算法；

[0016] A3) 语句解析模块判断 SQL 语句是否合法，若否，过程终止，若合法，进入下一步；

[0017] A4) 语句解析模块生成 SQL 重写记录，该记录记载了加密的表列和相应的加密算法名称，以及加密后的数据类型；

[0018] A5) 重写记录由加解密表列管理模块进行存储；

[0019] A6) 语句解析模块将 SQL 重写记录返回给 SQL 重写主模块，SQL 重写主模块再将重写记录和待重写的 SQL 语句交由重写执行模块执行；

[0020] A7) 重写执行模块根据重写记录将含有加密列数据表的 SQL 语句重写成标准 SQL 语句，修改列数据类型为加密后的数据类型，然后将重写后的 SQL 请求语句送交 SQL 重写主模块；

[0021] A8) 重写后的 SQL 请求语句被送往数据库系统创建数据表。

[0022] 所述的使用方法，数据的插入过程包括：

[0023] B1) SQL 重写主模块将执行数据插入的 SQL 语句输入语句解析模块；

[0024] B2) 语句解析模块根据加解密表列管理模块的记录，逐个检查每个数据列是否已记载在 SQL 重写记录中，若否，不做任何重写，执行 B6；若为是，则该数据列需要进行加密处理，进入下一步；

[0025] B3) 语句解析模块将需要加密的表列和相应的加密算法名发送给 SQL 重写主模块；

[0026] B4) SQL 重写主模块将包含需加密表列数据的 SQL 语句发送给重写执行模块，重写执行模块调用数据加解密模块进行加密，得到加密后的表列数据；

[0027] B5) 重写执行模块将 SQL 语句中的需加密的表列数据替换为加密后的表列数据，并返回给 SQL 重写主模块；

[0028] B6) SQL 重写主模块将数据插入语句送往数据库系统。

[0029] 所述的使用方法，数据的查询过程包括：

[0030] C1) SQL 重写主模块接收从数据库系统查询数据的 SQL 请求语句，并发送给语句解析模块；

[0031] C2) 语句解析模块根据加解密表列管理模块的记录，逐个检查待查询的数据列是否记录在该记录中，若否，执行步骤 C5；若为是，则该数据列需要进行解密处理，进入下一步；

[0032] C3) 语句解析模块将需要解密的表列和相应的加密算法名发送给 SQL 重写主模块；

[0033] C4) SQL 重写主模块将需要解密的数据表列列为待处理项；

[0034] C5) SQL 重写主模块将 SQL 查询语句发往数据库得到查询结果；

[0035] C6) 对于查询结果，SQL 重写主模块检查是否包含有待处理项，若否，执行步骤 C8；

若为是，进入下一步；

[0036] C7)SQL 重写主模块调用数据加解密模块中相应的加密算法，将待处理项进行解密；

[0037] C8)SQL 重写主模块返回最终的查询结果。

[0038] 本发明的技术效果：本发明采用 SQL 重写技术，在数据库系统外部对数据进行加解密，从而避免数据库系统加解密开销。SQL 重写保证数据加解密对应用系统的透明，将 SQL 请求直接作用在数据库实体数据表列上。SQL 重写可保证加解密算法和明文数据仅对应用系统开放，杜绝了数据库系统对明文敏感数据的访问。同时，加解密流程与数据库系统相脱离，对数据库系统不做任何修改。基于 SQL 重写的数据库加解密方法可强化加密、查询、传输、解密整个操作流程的安全性和效率性。

[0039] 总之，本发明解决了数据库加密中数据库系统负载过重、明文暴露、传输泄露的问题，提高了数据库加密的安全性、可靠性和有效性。

附图说明

[0040] 图 1 为子模块调用示意图。

[0041] 图 2 为创建数据表流程示意图。

[0042] 图 3 为插入数据流程示意图。

[0043] 图 4 为查询数据流程示意图。

具体实施方式

[0044] 为了解决数据库系统加解密的大量开销问题，简化数据库处理流程，降低数据库系统负载，本发明采用在数据库外部对数据进行加解密的方式，该方式既保证了面向业务系统的透明性，也减缓了数据库系统的加解密压力。另外，由于数据库安全的防范重点在于杜绝数据库管理人员从内部窃取，应避免明文暴露在数据库系统中，外部加密方式可实现加解密过程脱离数据库系统运行环境。

[0045] SQL(Structed Query Language，结构化查询语言）重写技术是在 SQL 请求语句从应用系统发出，在数据库系统执行之前，对语句进行改写，已达到查询性能优化等目的。SQL 重写可以保证数据库实体表列直接接受 SQL 请求，保证加解密算法和数据仅对应用系统开放，杜绝了数据库系统对明文敏感数据的访问。另外，加解密流程与数据库系统相脱离，对数据库系统不做任何修改，仅需针对不同数据库系统建立不同的 SQL 重写机制。基于 SQL 重写的数据库加密方法可强化加密、查询、传输、解密整个操作流程的安全性和效率性。

[0046] 一种基于 SQL 重写的数据库外部加解密方法，使得数据加解密脱离数据库系统环境。该方法包括 SQL 重写主模块、语句解析模块、语法规则管理模块、加解密表列管理模块、重写执行模块以及数据加解密模块。

[0047] 创建数据表时，SQL 重写主模块接收用户发出的 SQL 请求语句，调用语句解析模块确定待重写的 SQL 请求语句片段。语句解析模块根据 SQL 请求类型，调用语法规则管理模块以获得解析方法。语句解析模块生成加密表列重写记录，记载入加解密表列管理模块。SQL 重写主模块将重写记录和待重写 SQL 语句输入重写执行模块，由重写执行模块执行 SQL 重写。完成整个重写过程后，SQL 重写主模块将重写后的 SQL 请求发往数据库系统。

[0048] 插入数据时，SQL 重写主模块接收用户发出的 SQL 请求语句，调用语句解析模块确定待重写的 SQL 请求语句片段。语句解析模块根据 SQL 请求类型，调用语法规则管理模块以获得解析方法。语句解析模块在加解密表列管理中查询是否有与插入数据相对应的重写记录。若有，表明插入的数据需进行加密。SQL 重写主模块将重写记录和待重写的插入语句输入重写执行模块，由重写执行模块调用数据加解密模块对插入数据加密，执行 SQL 重写。SQL 重写主模块将重写后的 SQL 请求发往数据库系统。

[0049] 查询数据时，SQL 重写主模块接收用户发出的 SQL 请求语句并输入语句解析模块。语句解析模块根据 SQL 请求类型，调用语法规则管理模块以获得解析方法。语句解析模块在加解密表列管理中查询是否有与查询数据相对应的重写记录。若有，表明查询返回的数据需进行解密。SQL 重写主模块根据重写记录，调用数据加解密模块对查询返回结果进行解密，然后将结果返回给用户。

[0050] 下面通过借助实施例和附图更加详细地说明本发明，但以下实施例仅是说明性的，本发明的保护范围并不受这些实施例的限制。

[0051] 本发明提供一种基于 SQL 重写的数据库加解密方法，其子模块调用关系示意图如图 1 所示，包括 SQL 重写主模块、语句解析模块、语法规则管理模块、加解密表列管理模块、重写执行模块以及数据加解密模块。

[0052] 所述 SQL 重写主模块接收应用系统发送的 SQL 请求语句，接收数据库系统返回的执行结果。在这一过程中，根据加解密需求对其他模块进行调度，并将最终语句执行结果返回给应用系统。

[0053] 所述语句解析模块负责对 SQL 语句进行语法和语义检查，以确定 SQL 语句是否需要重写和需要重写的部分。

[0054] 所述语法规则管理模块内定义了和加解密相关的 SQL 语句关键字，供语句解析模块参考。

[0055] 所述加解密表列管理模块对数据库中已加密的表列和加解密算法进行记录。

[0056] 所述重写执行模块受 SQL 重写主模块调用，执行 SQL 语句的重写，并与数据加解密模块进行数据通信。

[0057] 所述数据加解密模块负责对输入值按照给定的加解密算法进行加密或者解密。

[0058] 为了进一步阐述加解密的 SQL 重写过程，根据 SQL 请求语句的类型，对整个方法的运作模式进行更具体的阐述。

[0059] 图 2 描述了 SQL 语句创建数据表，需要对某些表列进行加密的详细流程：

[0060] (A1) SQL 重写主模块将创建数据表的 SQL 语句输入语句解析模块。创建数据表的 SQL 请求语句中在需要加密的列的前面有两个关键字：ENC(Encrypt，即加密）和加密算法名。ENC 指明该列需要加密。语法规则管理模块对关键字 ENC 和加密算法名做了登记。

[0061] 该请求语句：

[0062]

```
CREATE TABLE 表名
(
  列名称 1 数据类型 1,
  ENC 加密算法 1 列名称 2 数据类型 2,
  ENC 加密算法 2 列名称 3 数据类型 3,
  ……
)
```

[0063] (A2) 语句解析模块调用语法规则管理模块获知 ENC 和加密算法名。

[0064] (A3) 语句解析模块判断 SQL 语句是否合法，若合法，进入下一步；若否，过程终止。

[0065] (A4) 语句解析模块生成 SQL 重写记录。该记录记载了加密的表列和相应的加密算法名称，以及加密后的数据类型。

[0066] 该重写记录对加密列 2，包含加密后数据类型 2’，对加密列 3 包含加密后数据类型 3’。

[0067] (A5) 重写记录由加解密表列管理模块进行存储。

[0068] (A6) 语句解析模块将 SQL 重写记录返回给 SQL 重写主模块，SQL 重写主模块再将重写记录和待重写的 SQL 语句交由重写执行模块执行。

[0069] (A7) 重写执行模块根据重写记录将 ENC 关键字和加密算法名去除，修改列数据类型为加密后的数据类型，完成 SQL 的重写，然后将重写后的 SQL 请求语句送交 SQL 重写主模块。

[0070] 该重写后的 SQL 语句为：

[0071]

```
CREATE TABLE 表名
(
  列名称 1 数据类型 1,
  列名称 2 加密后数据类型 2’,
  列名称 3 加密后数据类型 3’,
  ……
)
```

[0072] (A8) 重写后的 SQL 请求语句被送往数据库系统创建数据表。

[0073] 图 3 描述了 SQL 语句插入数据，其中某些表列需要加密的详细流程：

[0074] (B1)SQL 重写主模块将执行数据插入的 SQL 语句输入语句解析模块。

[0075] 该 SQL 语句为：

[0076] INSERT INTO 表名

[0077] (列 1,…, 列 i,…)

[0078] VALUES(值 1,…, 值 i,…)

[0079] 其中 i 的取值为所有列的序号。

[0080] (B2) 语句解析模块通过加解密表列管理模块，检查“列 i”是否已记载在 SQL 重写记录中。若是，执行下一步；若否，不做任何重写，执行 (B6)。

[0081] (B3) 语句解析模块将“列 i”的重写记录发送给 SQL 重写主模块。

[0082] (B4)SQL 重写主模块将“列 i”的重写记录和待重写 SQL 语句发送给重写执行模块。重写执行模块根据“列 i”对应的加密算法名，调用加解密模块进行加密，得到返回值“值 i’”。

[0083] 替换后的 SQL 语句为：

[0084] INSERT INTO 表名

[0085] (列 1,…, 列 i,…)

[0086] VALUES(值 1,…, 值 i’,…)

[0087] (B5) 重写执行模块将 SQL 请求语句中的“值 i”替换为“值 i’”，完成 SQL 重写，并返回给 SQL 重写主模块。

[0088] (B6)SQL 重写主模块将数据插入语句送往数据库系统。

[0089] 图 4 描述了采用 SQL 语句查询数据，返回的表列有加密数据的详细流程。

[0090] (C1) 语句解析模块从 SQL 重写主模块接收从数据库系统查询数据的 SQL 请求语句 (SELECT 语句)。

[0091] 该 SQL 语句为：

[0092] SELECT 列 1,…, 列 i,…

[0093] FROM 表名

[0094] (C2) 语句解析模块检查 SELECT 的“列 i”是否记录在加密表列管理模块中。若是，执行下一步：若否，执行 (C5)

[0095] (C3) 语句解析模块将“列 i”的重写记录返回给 SQL 重写主模块。

[0096] (C4)SQL 重写主模块将“列 i”列为待处理项，表明需对该列查询结果进行解密处理。该查询结果为：(值 1,…, 值 i,…)

[0097] (C5)SQL 重写主模块将 SELECT 语句发往数据库得到查询结果。

[0098] (C6) 对于查询结果，SQL 重写主模块检查是否记录了待处理项“列 i”，若是，执行下一步；若否，执行 (C8)。

[0099] (C7)SQL 重写主模块对相应的“值 i”，采用重写记录中的加密算法，调用加解密模块中进行解密。

[0100] (C8)SQL 重写主模块将解密后的结果返回。

[0101] 应当明确，所描述的实施例仅是本发明的一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造新劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

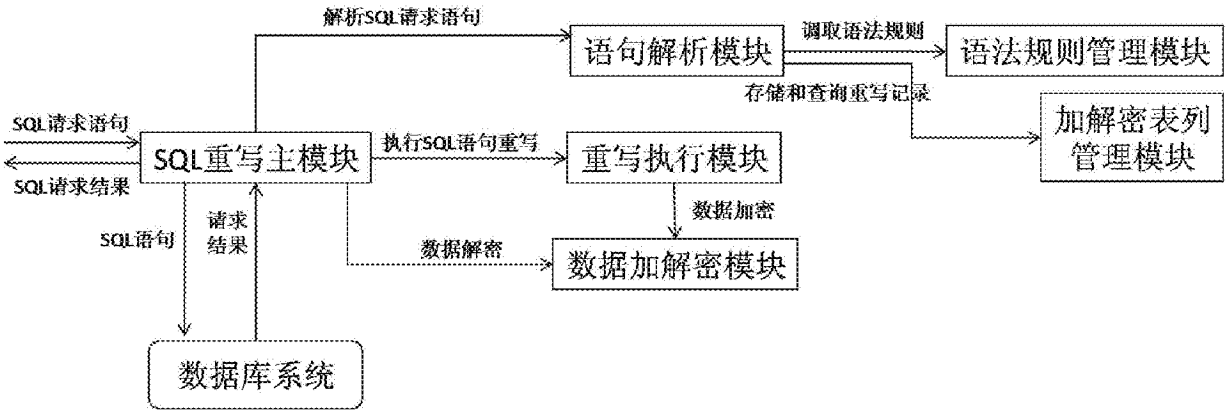

解析SQL请求语句
语句解析模块
调取语法规则
语法规则管理模块
存储和查询重写记录
加解密表列管理模块
SQL请求语句
SQL请求结果
SQL重写主模块
执行SQL语句重写
重写执行模块
数据加密
SQL语句
请求结果
数据解密
数据加解密模块
数据库系统

图 1

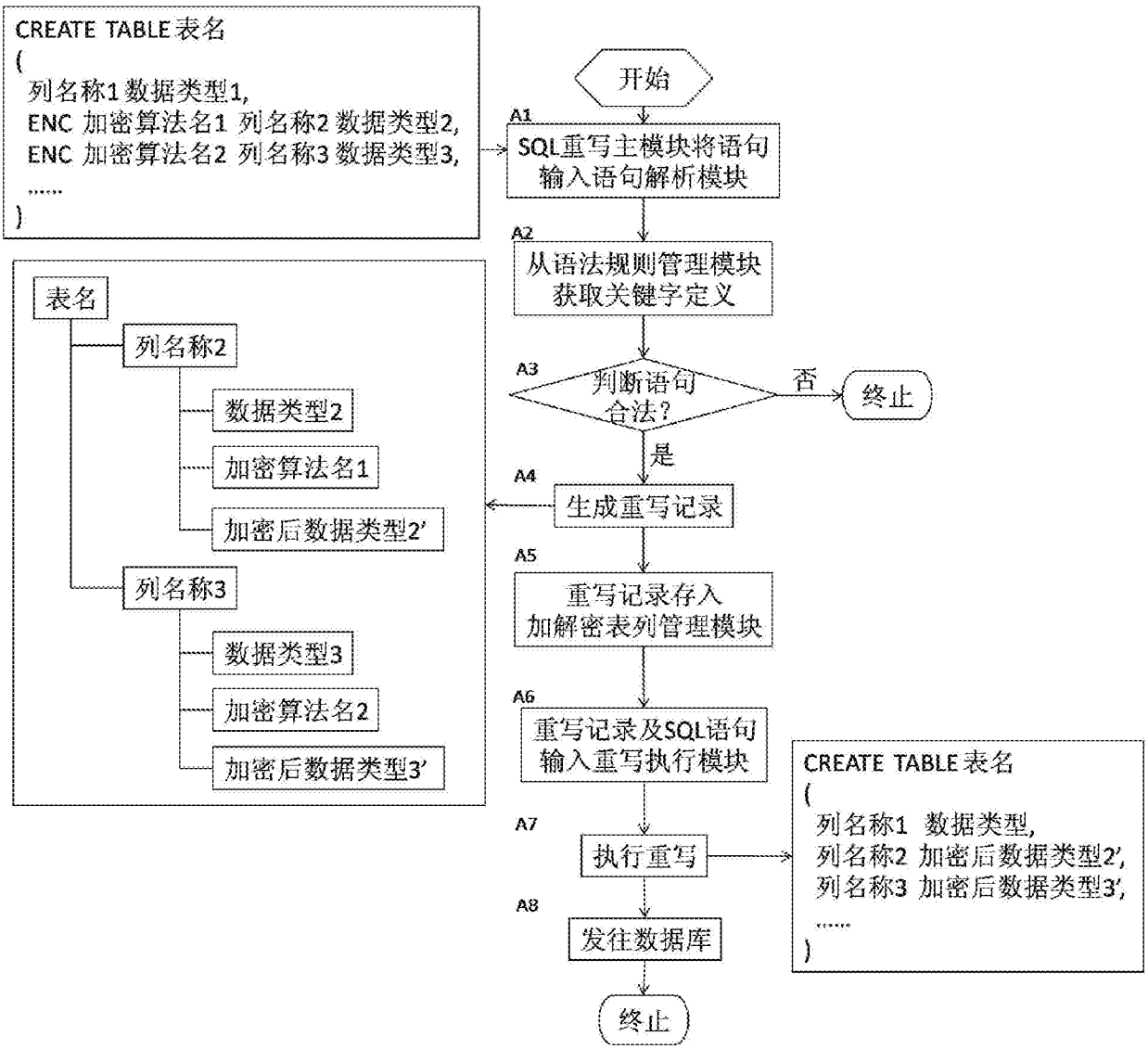

CREATE TABLE表名
(
列名称1 数据类型1,
ENC 加密算法名1 列名称2 数据类型2,
ENC 加密算法名2 列名称3 数据类型3,
.....
)
表名
列名称2
数据类型2
加密算法名1
加密后数据类型2'
列名称3
数据类型3
加密算法名2
加密后数据类型3'
开始
A1
SQL重写主模块将语句输入语句解析模块
A2
从语法规则管理模块获取关键字定义
A3
判断语句合法?
否
终止
是
A4
生成重写记录
A5
重写记录存入加解密表列管理模块
A6
重写记录及SQL语句输入重写执行模块
A7
执行重写
A8
发往数据库
终止
CREATE TABLE表名
(
列名称1 数据类型,
列名称2 加密后数据类型2',
列名称3 加密后数据类型3',
.....
)

图 2

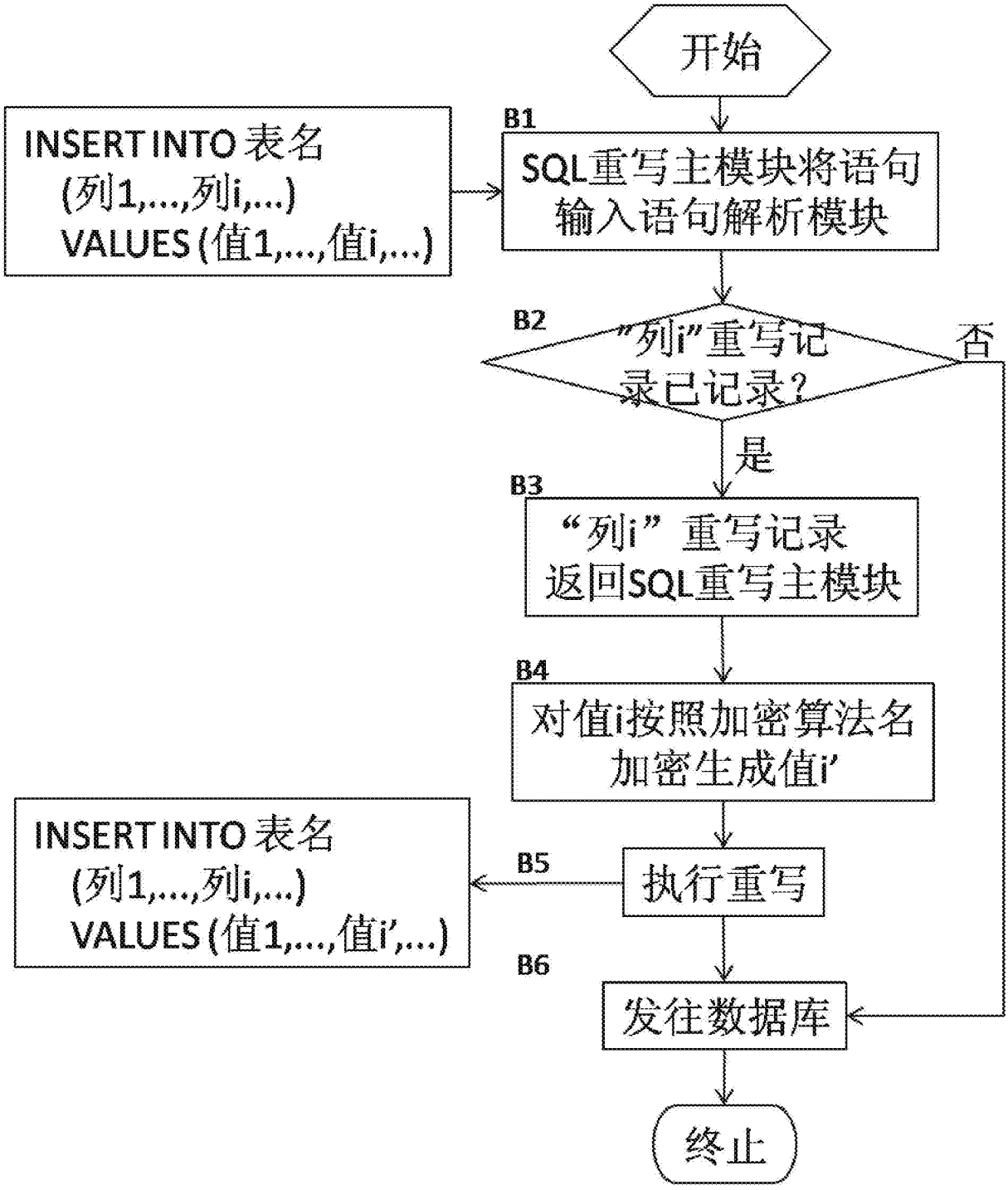

开始
INSERT INTO 表名
(列1,...,列i,...)
VALUES (值1,...,值i,...)
B1
SQL重写主模块将语句
输入语句解析模块
B2
"列i"重写记
录已记录?
否
是
B3
"列i" 重写记录
返回SQL重写主模块
B4
对值i按照加密算法名
加密生成值i'
INSERT INTO 表名
(列1,...,列i,...)
VALUES (值1,...,值i',...)
B5
执行重写
B6
发往数据库
终止

图 3

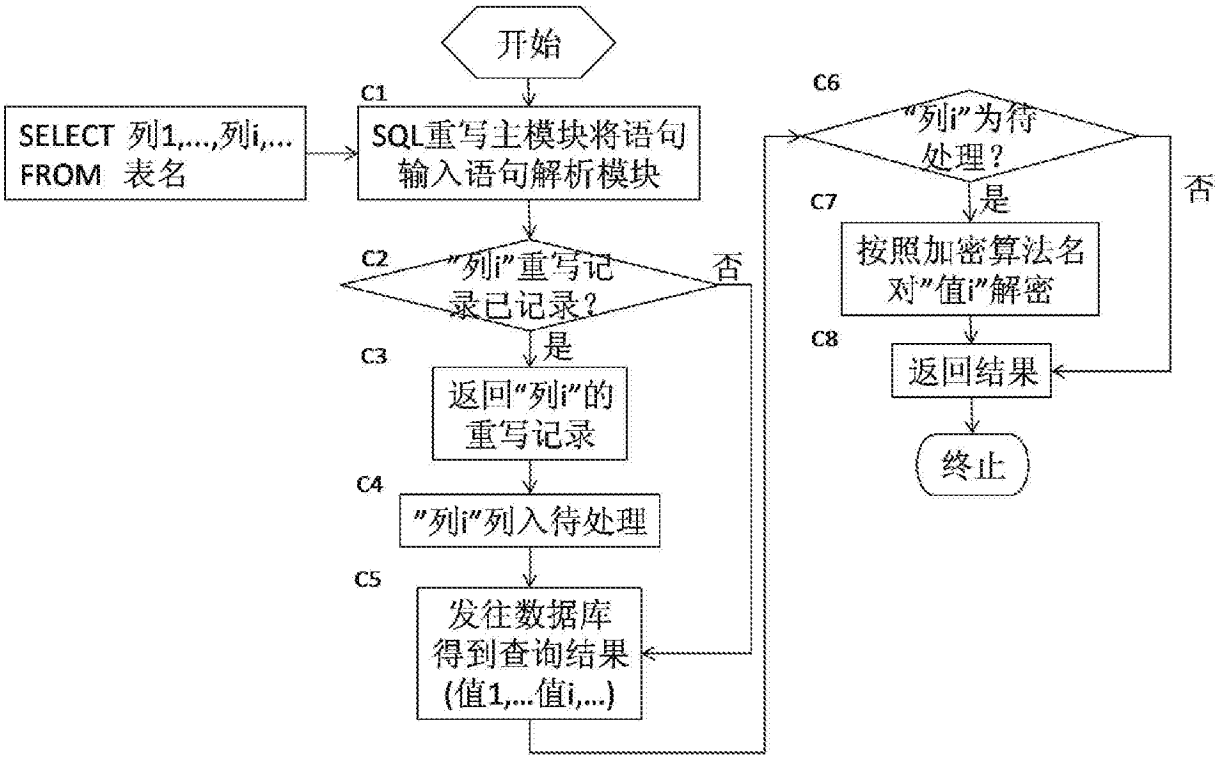

开始
C1
SELECT 列1,...,列i,...
FROM 表名
SQL重写主模块将语句输入语句解析模块
C2
"列i"重写记录已记录?
否
是
C3
返回"列i"的重写记录
C4
"列i"列入待处理
C5
发往数据库得到查询结果(值1,...值i,...)
C6
"列i"为待处理?
否
是
C7
按照加密算法名对"值i"解密
C8
返回结果
终止

图 4