

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



PCT



(43) 国际公布日
2007 年 9 月 7 日 (07.09.2007)

(10) 国际公布号
WO 2007/098687 A1

(51) 国际专利分类号:

G09C 1/00 (2006.01) H04L 9/28 (2006.01)
G06F 12/16 (2006.01)

(21) 国际申请号:

PCT/CN2007/000617

(22) 国际申请日:

2007 年 2 月 27 日 (27.02.2007)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

200610041863.9

2006 年 3 月 2 日 (02.03.2006) CN

(71) 申请人 (对除美国外的所有指定国): 西安西电捷通
无线网络通信有限公司(CHINA IWNCOMM CO.,
LTD.) [CN/CN]; 中国陕西省西安市高新区科技二路
68 号西安软件园秦风阁 A201, Shaanxi 710075 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): 鹿甲寅(LU, Jiayin)
[CN/CN]; 中国陕西省西安市高新区科技二路 68 号
西安软件园秦风阁 A201, Shaanxi 710075 (CN)。 曹
军(CAO, Jun) [CN/CN]; 中国陕西省西安市高新区科
技二路 68 号西安软件园秦风阁 A201, Shaanxi 710075

(CN)。 颜湘(YAN, Xiang) [CN/CN]; 中国陕西省西
安市高新区科技二路 68 号西安软件园秦风阁 A201,
Shaanxi 710075 (CN)。 黄振海(HUANG, Zhenhai)
[CN/CN]; 中国陕西省西安市高新区科技二路 68 号
西安软件园秦风阁 A201, Shaanxi 710075 (CN)。

(74) 代理人: 北京集佳知识产权代理有限公司(UNI-
TALLEN ATTORNEYS AT LAW); 中国北京市朝阳区
建国门外大街 22 号赛特广场 7 层, Beijing 100004
(CN)。

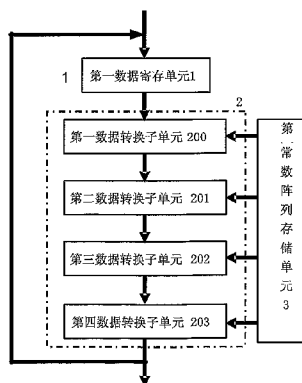
(81) 指定国 (除另有指明, 要求每一种可提供的国家保
护): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR,
BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK,
DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM,
GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN,
KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA,
MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD,
SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ,
UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA,
SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY,
KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH,
CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS,

[见续页]

(54) Title: ENCRYPTION AND DECRYPTION PROCESSING METHOD OF ACHIEVING SMS4 CRYPTOGRAPHIC ALGORITHM AND SYSTEM THEREOF

(54) 发明名称: 一种实现 SMS4 密码算法中加解密处理的方法及系统



1 THE FIRST DATA REGISTERING UNIT
3 THE FIRST CONSTANT ARRAY STORAGE UNIT
200 THE FIRST DATA CONVERSION SUBUNIT
201 THE SECOND DATA CONVERSION SUBUNIT
202 THE THIRD DATA CONVERSION SUBUNIT
203 THE FOURTH DATA CONVERSION SUBUNIT

(57) Abstract: An encryption and decryption processing method of achieving SMS4 cryptographic algorithm and a system thereof are disclosed. Firstly, the method prepares constant arrays, inputs the external data into a data registering unit and deals with the first data conversion; secondly, deals with the second data conversion; thirdly, repeats the second data conversion, until completing all the prescribed data conversion, and then achieving the results of repeating encryption and decryption processing.

[见续页]



IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR),
OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML,
MR, NE, SN, TD, TG)。

所引用双字母代码及其它缩写符号，请参考刊登在每
期PCT公报期刊起始的“代码及缩写符号简要说明”。

本国际公布：

— 包括国际检索报告。

(57) 摘要：

一种实现 SMS4 密码算法中加解密处理的方法及系统，首先是准备常数阵列，将外部数据输入数据寄存单元，进行首次数据转换处理；然后进行再次数据转换处理；再后重复再次数据转换处理，直至完成所有规定的的数据转换处理过程，得到循环加解密数据处理结果。本发明能够减少数据转换处理的循环次数，从而提高了加解密的效率。此外，采用本发明设计集成电路，可大大降低系统的干扰及成本。

一种实现 SMS4 密码算法中加解密处理的方法及系统

本申请要求于 2006 年 3 月 2 日提交中国专利局、申请号为 200610041863.9、发明名称为“一种实现 SMS4 密码算法中加解密处理的方法”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明主要应用于信息技术领域，具体涉及一种实现 SMS4 密码算法中加解密处理的方法及系统。

背景技术

实现 SMS4 加密算法的关键部件是密钥扩展部件和加解密部件。密钥扩展部件与加解密部件的内部结构及处理过程基本相同。加解密部件主要由三部分构成，即数据寄存部件、常数阵列存储部件、数据转换部件。具体如下：

数据寄存部件主要由通用触发器构成，用于数据的寄存。在一个时钟周期内，该部件所寄存的数据是不改变的。通用触发器是在时钟上沿或下沿把数据输入端的数据输入至触发器输出端，而在其他时刻触发器输出端的数据不发生变化的数据暂存器件。

常数阵列存储部件是存储常数阵列的存储部件。现有技术中的常数阵列一般是加解密处理之前已经准备好的宽度为 32 比特、深度为 32 的数据阵列。常数阵列存储部件的数据按照地址的高低顺序排列，可命名为 rk0, rk1, ..., rk31。

数据转换部件是按照密码算法要求进行数据处理的部件。例如，按照国家的 SMS4 密码算法要求进行数据处理，数据转换部件完成的操作中只有一次密码算法所规定的合成置换。

目前，按照 SMS4 密码算法要求进行加解密数据处理的方法如下：

1) 将外部数据输入数据寄存部件。外部数据输入到数据寄存部件后，数据寄存部件的输出端输出数据。例如，128 位 (bit) 的外部数据，分为 4 个 32bit 的数据块，可分别命名为 A0、A1、A2、A3。经数据寄存部件后输出端的数据仍为 128bit，分为 4 个 32bit 的数据块，分别相应地命名为 a0、a1、a2、a3。

2) 进行数据转换处理；

将数据寄存部件的输出端的数据输入至数据转换部件进行数据转换处理。例如，数据寄存部件的输出端的数据 a0、a1、a2、a3 经数据转换部件转换为

128bit 的数据 C0、C1、C2、C3。

3) 进行再次数据转换处理;

将前次数据转换处理后的数据再次存至数据寄存部件,然后将数据寄存部件输出端的数据再次输入数据转换部件,进行再次数据转换处理。

4) 重复再次数据转换处理,得到最终的数据处理结果。

对 128bit 的外部数据,再次数据转换处理须循环处理 30 次,即数据转换处理总共要进行 32 次,才能得到最终的数据处理结果。

上述现有技术通过加解密处理之前准备宽度为 32bit、深度为 32 的常数阵列,以及通过数据转换部件完成只有一次密码算法所规定的合成置换的操作,从而使得数据转换处理的循环次数较多。例如,加密 128bit 数据,至少需运行 32 个数据转换处理周期才能得到最终数据处理结果。

此外,上述现有技术加解密效率较低。加密效率即单位时间内加密的数据数量。例如,加密 128bit 数据需要进行数据转换处理 32 次。由于目前实际应用中的时钟频率一般都较低,使得单位时间内加密的数据数量少,效率低。如果指定加密效率,则需提高时钟频率,而实际应用中的时钟频率往往很难提高,所以实际加密效率仍然较低。如果要提高时钟频率,还会导致现有集成电路的设计、实施困难;信号完整性不好;设计成本较高。此外,现有技术方法设计的集成电路,应用于系统中,也会导致印制电路板(PCB, Printed circuit board)成本增加;PCB 设计困难,产品实施困难;以及系统中的干扰很大,会影响其他设备、器件的正常、高效工作。

发明内容

本发明提供一种实现 SMS4 密码算法中加解密处理的方法及系统,能够减少数据转换处理的循环次数,提高加密效率。

本发明的技术解决方案是:

一种实现 SMS4 密码算法中加解密处理的方法,该方法包括循环加解密数据处理的步骤,包括:

安排第一常数阵列数据的宽度和深度,相同深度的数据构成一行,存储所述第一常数阵列;

在第一时钟周期的上沿或下沿,输出寄存的外部数据;

在该第一时钟周期内, 对所述存储的第一常数阵列中的第一行第一个数据, 与所述寄存的外部数据进行数据转换处理, 获得第一次第一转换数据;

对所述存储的第一常数阵列中的第一行第二个数据, 与所述的第一次第一转换数据进行数据转换处理, 获得第一次第二转换数据;

依此方式, 直至将所述存储的第一常数阵列中第一行的所有数据顺序完成数据转换处理, 获得第一次转换处理数据;

在第二个时钟周期的上沿或下沿到来的时刻, 将第一次转换处理数据寄存起来;

在该第二时钟周期内, 对所述存储的第一常数阵列中的第二行第一个数据, 与所述寄存的第一次转换处理数据进行数据转换处理, 获得第二次第一转换数据;

对所述存储的第一常数阵列中的第二行第二个数据, 与所述的第二次第一转换数据进行数据转换处理, 获得第二次第二转换数据;

依此方式, 直至将所述存储的第一常数阵列中第二行的所有数据顺序完成数据转换处理, 获得第二次转换处理数据;

重复上述数据转换处理过程, 直至完成所有深度个数的数据转换处理过程, 得到循环加解密数据处理结果。

优选的, 所述的第一常数阵列满足以下条件:

数据按照地址由高到低的顺序排列并存储;

根据数据转换处理次数安排所述第一常数阵列数据的宽度和深度, 且宽度与深度的乘积为 1024;

相同深度的数据构成一行。

优选的: 所述的循环加解密数据处理步骤之前还包括第一附加加解密数据处理的步骤, 包括:

根据第一附加加解密数据处理步骤中数据转换处理的次数安排第二常数阵列数据的宽度, 第二常数阵列数据的深度为 1, 且相同深度的数据构成一行, 存储所述第二常数阵列;

在时钟周期的上沿或下沿, 输出寄存的外部数据;

在该时钟周期内, 对所述存储的第二常数阵列中的第一个数据, 与所述寄

存的外部数据进行数据转换处理, 获得第一转换数据;

对所述存储的第二常数阵列中的第二个数据, 与所述的第一转换数据进行数据转换处理, 获得第二转换数据;

依此方式, 直至将第一附加加解密数据处理步骤中所述存储的第二常数阵列中的所有数据顺序完成数据转换处理, 得到第一附加加解密数据处理结果; 以第一附加加解密数据处理结果作为循环加解密数据处理中的外部数据。

优选的, 所述的第一常数阵列和第二常数阵列满足以下条件:

所述第二常数阵列数据宽度为第一附加加解密数据处理步骤中数据转换的次数乘以 32, 所述第二常数阵列数据深度为 1, 确定所述第二常数阵列数据宽度与深度的乘积;

所述第二常数阵列数据宽度与深度的乘积, 与所述第一常数阵列数据宽度与深度的乘积之和为 1024。

优选的, 所述的循环加解密数据处理步骤之后还包括第二附加加解密数据处理的步骤, 包括:

根据第二附加加解密数据处理步骤中数据转换次数安排第三常数阵列数据的宽度, 第三常数阵列数据的深度为 1, 且相同深度的数据构成一行, 存储所述第三常数阵列;

将所述循环加解密数据处理结果寄存起来, 在时钟周期的上沿或下沿, 输出寄存的数据;

在该时钟周期内, 对所述存储的第三常数阵列中的第一个数据, 与所述寄存的外部数据进行数据转换处理, 获得第一转换数据;

对所述存储的第三常数阵列中的第二个数据, 与所述的第一转换数据进行数据转换处理, 获得第二转换数据;

依此方式, 直至将第二附加加解密数据处理步骤中所述存储的第三常数阵列中的所有数据顺序完成数据转换处理, 得到第二附加加解密数据处理结果; 所述的第二附加加解密数据处理结果即为最终加解密数据处理结果。

优选的, 所述第一常数阵列、第二常数阵列、及第三常数阵列满足以下条件:

所述第二常数阵列数据宽度为第一附加加解密数据处理步骤中数据转换

的次数乘以 32, 所述第二常数阵列数据深度为 1, 确定所述第二常数阵列数据宽度与深度的乘积;

所述第三常数阵列数据宽度为第二附加加解密数据处理步骤中数据转换的次数乘以 32, 所述第三常数阵列数据深度为 1, 确定所述第三常数阵列数据宽度与深度的乘积;

所述第二常数阵列数据宽度与深度的乘积, 与所述第三常数阵列数据宽度与深度的乘积, 及所述第一常数阵列数据宽度与深度的乘积之和为 1024。

优选的, 所述的循环加解密数据处理步骤之后还包括第二附加加解密数据处理的步骤, 包括:

根据第二附加加解密数据处理步骤中数据转换次数安排第三常数阵列数据的宽度, 第三常数阵列数据的深度为 1, 且相同深度的数据构成一行, 存储所述第三常数阵列;

将所述循环加解密数据处理结果寄存起来, 在时钟周期的上沿或下沿, 输出寄存的数据;

在该时钟周期内, 对所述存储的第三常数阵列中的第一个数据, 与所述寄存的外部数据进行数据转换处理, 获得第一转换数据;

对所述存储的第三常数阵列中的第二个数据, 与所述的第一转换数据进行数据转换处理, 获得第二转换数据;

依此方式, 直至将第二附加加解密数据处理步骤中所述存储的第三常数阵列中的所有数据顺序完成数据转换处理, 得到第二附加加解密数据处理结果; 所述的第二附加加解密数据处理结果即为最终加解密数据处理结果。

优选的, 所述的第一常数阵列和第三常数阵列满足以下条件:

所述第三常数阵列数据宽度为第二附加加解密数据处理步骤中数据转换的次数乘以 32, 所述第三常数阵列数据深度为 1, 确定所述第三常数阵列数据宽度与深度的乘积;

所述第三常数阵列数据宽度与深度的乘积, 与所述第一常数阵列数据宽度与深度的乘积之和为 1024。

一种实现 SMS4 密码算法中加解密处理的系统, 该系统包括循环加解密数据处理装置, 所述装置包括第一常数阵列存储单元、第一数据寄存单元、以及

第一数据转换单元, 所述第一数据转换单元包括 N 个数据转换子单元; 其中:

所述的第一常数阵列存储单元, 用于存储第一常数阵列, 以及在每一个时钟周期内, 顺序的将所述第一常数阵列的每一行数据分别对应输至第一数据转换单元的 N 个数据转换子单元;

所述的第一数据寄存单元, 用于寄存数据, 以及在每一个时钟周期的上沿或下沿, 将所述寄存的数据从输入端传送至输出端, 并于每一个时钟周期内, 将数据输至第一数据转换子单元;

所述的 N 个数据转换子单元, 用于在每一个时钟周期内, 依次进行数据转换处理, 并将获得的转换数据输至下一个数据转换子单元继续处理, 直至完成所有深度个数的数据转换处理过程, 得到循环加解密数据处理结果。

优选的, 所述的第一常数阵列满足以下条件:

数据的宽度和深度是根据数据转换子单元的个数 N 安排, 且数据宽度与深度的乘积为 1024, 相同深度的数据构成一行, 数据按照地址由高到低的顺序排列。

优选的, 还包括第一附加加解密数据处理装置, 所述装置包括第二常数阵列存储单元、第二数据寄存单元、以及第二数据转换单元, 所述第二数据转换单元包括 M 个数据转换子单元; 其中:

所述的第二常数阵列存储单元, 用于存储第二常数阵列, 以及在每一个时钟周期内, 顺序的将所述第二常数阵列的每一行数据分别对应输至第二数据转换单元的 M 个数据转换子单元;

所述的第二数据寄存单元, 用于寄存数据, 以及在每一个时钟周期的上沿或下沿, 将所述寄存的数据从输入端传送至输出端, 并于每一个时钟周期内, 将数据输至第二数据转换子单元;

所述的 M 个数据转换子单元, 用于在每一个时钟周期内, 依次进行数据转换处理, 并将获得的转换数据输至下一个数据转换子单元继续处理, 直至完成所有深度个数的数据转换处理过程, 得到第一附加加解密数据处理结果; 以第一附加加解密数据处理结果作为循环加解密数据处理中的寄存数据。

优选的, 所述的第一常数阵列和第二常数阵列满足以下条件:

该第二常数阵列数据的宽度和深度是根据第一附加加解密数据处理装置

中数据转换子单元的个数 M 安排, 且相同深度的数据构成一行; 所述第二常数阵列数据宽度为第一附加加解密数据处理装置中数据转换子单元个数 M 乘以 32, 所述第二常数阵列数据深度为 1, 确定所述第二常数阵列数据宽度与深度的乘积为 $M \times 32 \times 1$;

所述第二常数阵列数据宽度与深度的乘积 $M \times 32 \times 1$, 与所述第一常数阵列数据宽度与深度的乘积之和为 1024。

优选的, 还包括第二附加加解密数据处理装置, 所述装置包括第三常数阵列存储单元、第三数据寄存单元、以及第三数据转换单元, 所述第三数据转换单元包括 Q 个数据转换子单元; 其中:

所述的第三常数阵列存储单元, 用于存储第三常数阵列, 以及在每一个时钟周期内, 顺序的将所述第三常数阵列的每一行数据分别对应输至第三数据转换单元的 Q 个数据转换子单元; 该第三常数阵列数据的宽度和深度是根据数据转换子单元的个数 Q 安排的, 第三常数阵列数据的深度为 1, 且相同深度的数据构成一行;

所述的第三数据寄存单元, 用于寄存数据, 以及在每一个时钟周期的上沿或下沿, 将所述寄存的数据从输入端传送至输出端, 并于每一个时钟周期内, 将数据输至第三数据转换子单元;

所述的 Q 个数据转换子单元, 用于在每一个时钟周期内, 依次进行数据转换处理, 并将获得的转换数据输至下一个数据转换子单元继续处理, 直至完成所有深度个数的数据转换处理过程, 得到第二附加加解密数据处理结果; 所述的第二附加加解密数据处理结果即为最终加解密数据处理结果。

优选的, 所述第一常数阵列、第二常数阵列、及第三常数阵列满足以下条件:

所述第二常数阵列数据的宽度和深度是根据第一附加加解密数据处理装置中数据转换子单元的个数 M 安排, 且相同深度的数据构成一行; 该第二常数阵列数据宽度为第一附加加解密数据处理装置中数据转换子单元个数 M 乘以 32, 所述第二常数阵列数据深度为 1, 确定所述第二常数阵列数据宽度与深度的乘积为 $M \times 32 \times 1$;

所述第三常数阵列数据的宽度和深度是根据第二附加加解密数据处理装

置中的数据转换子单元的个数 Q 安排, 且相同深度的数据构成一行; 该第三常数阵列数据宽度为第二附加加解密数据处理装置中数据转换子单元个数 Q 乘以 32, 所述第三常数阵列数据深度为 1, 确定所述第三常数阵列数据宽度与深度的乘积为 $Q \times 32 \times 1$;

所述第二常数阵列数据宽度与深度的乘积 $M \times 32 \times 1$, 与所述第三常数阵列数据宽度与深度的乘积 $Q \times 32 \times 1$, 及所述第一常数阵列数据宽度与深度的乘积之和为 1024。

优选的, 还包括第二附加加解密数据处理装置, 所述装置包括第三常数阵列存储单元、第三数据寄存单元、以及第三数据转换单元, 所述第三数据转换单元包括 Q 个数据转换子单元; 其中:

所述的第三常数阵列存储单元, 用于存储第三常数阵列, 以及在每一个时钟周期内, 顺序的将所述第三常数阵列的每一行数据分别对应输至第三数据转换单元的 Q 个数据转换子单元;

所述的第三数据寄存单元, 用于寄存数据, 以及在每一个时钟周期的上沿或下沿, 将所述寄存的数据从输入端传送至输出端, 并于每一个时钟周期内, 将数据输至第三数据转换子单元;

所述的 Q 个数据转换子单元, 用于在每一个时钟周期内, 依次进行数据转换处理, 并将获得的转换数据输至下一个数据转换子单元继续处理, 直至完成所有深度个数的数据转换处理过程, 得到第二附加加解密数据处理结果; 所述的第二附加加解密数据处理结果即为最终加解密数据处理结果。

优选的, 所述的第一常数阵列和第三常数阵列满足以下条件:

所述第三常数阵列数据的宽度和深度是根据第二附加加解密数据处理装置中的数据转换子单元的个数 Q 安排, 且相同深度的数据构成一行; 该第三常数阵列数据宽度为第二附加加解密数据处理装置中数据转换子单元个数 Q 乘以 32, 所述第三常数阵列数据深度为 1, 确定所述第三常数阵列数据宽度与深度的乘积为 $Q \times 32 \times 1$;

所述第三常数阵列数据宽度与深度的乘积 $Q \times 32 \times 1$, 与所述第一常数阵列数据宽度与深度的乘积之和为 1024。

本发明实现 SMS4 密码算法中加解密处理的方法, 通过对常数阵列的安排

以及对应数据转换子单元的设置,能够减少数据转换处理的循环次数。由于单位时间内加密的数据数量大大增加,从而提高了加密的效率。例如,加密 128bit 的数据,若采用 4 个数据转换子单元,只需循环运行 8 个时钟周期就能输出最终数据处理结果。所以,在时钟频率相同的情况下,可以使加密效率提高 4 倍。

本发明实现 SMS4 密码算法中加解密处理的系统,在满足所要求加密效率的情况下,由于时钟频率仅为原来的 $1/n$,故时钟频率只需原来的 $1/n$ 。例如,加密 128bit 的数据,若采用 4 个数据转换子单元,时钟频率只需原来的 $1/4$ 。

此外,在相同处理效率的情况下,实现本发明方案的集成电路的设计、实施比较容易;信号的完整性大大优化;设计成本降低。此外,采用本发明设计集成电路,在满足所要求加密效率的情况下,由于时钟频率仅为原来的 $1/n$,故时钟频率只需原来的 $1/n$ 。在相同处理效率的情况下 PCB 成本降低;PCB 设计、产品易于实现;系统中的干扰降低,对其他设备、器件正常、高效工作的影响也大幅度降低。

附图说明

图 1 为本发明实施例一循环加解密数据处理示意图;

图 2 为本发明实施例二循环加解密数据处理示意图;

图 3 为本发明实施例三在循环加解密数据处理之前加有附加加解密数据处理示意图;

图 4 为本发明实施例四在循环加解密数据处理之后加有附加加解密数据处理示意图;

图 5 为本发明实施例五循环加解密数据处理之前、之后均加有附加加解密数据处理示意图。

具体实施方式

如图 1 所示,为本发明实施例一循环加解密数据处理示意图,主要包括第一数据寄存单元 1、第一常数阵列存储单元 3 及第一数据转换单元 2。

第一数据寄存单元 1 用于寄存外部数据及上一次数据转换处理的结果。第一数据寄存单元 1 一般可采用通用触发器,如 D 触发器、JK 触发器等。该类通用触发器是在时钟上沿或下沿把数据输入端的数据传至触发器的输出端,在

其他时刻触发器输出端的数据不发生变化的数据暂存器件,即在同一个数据转换处理周期内,第一数据寄存单元1所寄存的数据是不改变的。

第一数据转换单元2用于按照密码算法要求进行数据处理。例如,按照国家的SMS4密码算法要求进行数据处理,第一数据转换单元2完成的操作中只有一次密码算法所规定的合成置换。

第一常数阵列存储单元3用于存储常数阵列数据。本发明实施例一采用的常数阵列是密钥扩展处理所得到的结果数据,按照地址高低顺序排列,按照循环体中第一数据转换单元2的数据转换子单元的个数安排常数阵列对应的宽度和深度,并且宽度与深度的乘积为1024。例如,采用4个数据转换子单元,那么常数阵列的宽度是128bit,深度是8;若采用8个数据转换子单元,常数阵列的宽度则是256bit,深度是4。

参见图1,本发明实施例一循环加解密数据处理的实现步骤如下:

1、根据数据转换处理子单元的个数安排第一常数阵列数据的宽度和深度,相同深度的数据构成一行,存储所述第一常数阵列;

2、在第一时钟周期的上沿或下沿,输出寄存的外部数据;

3、在该第一时钟周期内,对所述存储的第一常数阵列中的第一行第一个数据,与所述寄存的外部数据进行数据转换处理,获得第一次第一转换数据;

对所述存储的第一常数阵列中的第一行第二个数据,与所述的第一次第一转换数据进行数据转换处理,获得第一次第二转换数据;

依此方式,直至将所述存储的第一常数阵列中第一行的所有数据顺序完成数据转换处理,获得第一次转换处理数据;

4、在第二个时钟周期的上沿或下沿到来的时刻,将第一次转换处理数据寄存起来;

在该第二时钟周期内,对所述存储的第一常数阵列中的第二行第一个数据,与所述寄存的第一次转换处理数据进行数据转换处理,获得第二次第一转换数据;

对所述存储的第一常数阵列中的第二行第二个数据,与所述的第二次第一转换数据进行数据转换处理,获得第二次第二转换数据;

依此方式,直至将所述存储的第一常数阵列中第二行的所有数据顺序完成

数据转换处理，获得第二次转换处理数据；

5、重复上述数据转换处理过程，直至完成所有深度个数的数据转换处理过程，得到循环加解密数据处理结果。

如图 2 所示，为本发明实施例二循环加解密数据处理示意图，包括第一数据寄存单元 1、第一常数阵列存储单元 3 及第一数据转换单元 2；其中，第一数据转换单元 2 包括 4 个数据转换子单元，即第一数据转换子单元 200、第二数据转换子单元 201、第三数据转换子单元 202、第四数据转换子单元 203。本发明实施例二中数据转换子单元的个数为 4，可以理解的是，对于数据转换子单元的个数是 32 的约数时，宜于采用循环加解密数据处理的方式实现，其处理过程与本发明实施例二类似。

参见图 2，本发明实施例二循环加解密数据处理的实现步骤如下：

1) 准备常数阵列。

(1) 将密钥扩展处理所得到的第一常数阵列数据按照地址高低顺序排列，存入常数阵列存储单元 3；

(2) 根据数据转换处理中数据转换处理单元 2 中数据转换子单元的个数安排对应宽度和深度，并且宽度与深度的乘积为 1024；

(3) 第一常数阵列中相同深度的数据构成一行。

2) 将外部数据输入第一数据寄存单元 1。

(1) 将外部数据输至第一数据寄存单元 1 的输入端；

(2) 在时钟上沿或下沿，把第一数据寄存单元 1 输入端的数据传送至其输出端。

3) 进行首次数据转换处理。

(1) 在该时钟周期内，将第一常数阵列存储单元 3 所存储第一常数阵列的第一行对应的数据分别输至第一数据转换单元 2 中所有的数据转换子单元 200 - 203；

(2) 在同一个时钟周期内，第一数据寄存单元 1 输出端的数据输入第一个数据转换子单元 200 进行数据转换处理；第一个数据转换子单元 200 输出的数据再输入到下一个数据转换子单元 201 进行数据转换处理；依此方式，直至数据转换单元 2 中所有的数据转换单元子 200 - 203 顺序完成数据转换处理。

4) 进行再次数据转换处理。

(1) 在下一个时钟沿到来的时刻, 将前次数据转换处理的数据存至第一数据寄存单元 1;

(2) 在该时钟周期内, 将第一常数阵列存储单元 3 所存储第一常数阵列的下一行对应的数据分别输至第一数据转换单元 2 中所有的数据转换子单元 200 - 203;

(3) 在同一个时钟周期内, 第一数据寄存单元 1 输出端的数据输入第一个数据转换子单元 200 进行数据转换处理; 第一个数据转换子单元 200 输出的数据再输入到下一个数据转换子单元 201 进行数据转换处理; 依此方式, 直至第一数据转换单元 2 中所有的数据转换子单元 200 - 203 顺序完成数据转换处理。

5) 重复再次数据转换处理。

重复再次数据转换处理过程, 直至完成所有规定的的数据转换处理过程, 得到循环加解密数据处理结果。

附加加解密数据处理用于补充完成循环加解密数据处理未完成的数据转换处理, 尤其是当第一数据转换单元 2 中数据转换子单元的个数不是 32 的约数时, 可通过循环加解密数据处理与附加加解密数据处理共同完成数据转换处理。针对这种情况, 下面通过实施例三至五具体说明。

如图 3 所示, 为本发明实施例三在循环加解密数据处理之前增加附加加解密数据处理示意图, 包括第一附加加解密数据处理装置 501 和循环加解密数据处理装置 4。其中, 该循环加解密数据处理装置 4 的组成同上述实施例二; 该第一附加加解密数据处理装置 501 包括第二数据寄存器 101、第二常数阵列存储单元 301、以及第二数据转换单元 21, 其中该第二数据转换单元 21 包括第一数据转换子单元 210 和第二数据转换子单元 211 等。

参见图 3, 在循环加解密数据处理之前增加附加加解密数据处理的实现步骤如下:

1) 准备常数阵列;

(1) 将密钥扩展处理所得到的第二常数阵列数据按照地址高低顺序排列, 存入第二常数阵列存储单元 301;

(2) ① 确定循环加解密数据处理中第一常数阵列的宽度和深度:

根据循环加解密数据处理中第一数据转换单元 2 中数据转换子单元的个数 N 安排对应宽度和深度, 得到循环加解密数据处理中第一常数阵列数据宽度与深度的乘积;

② 确定附加加解密数据处理中第二常数阵列数据的宽度和深度:

根据附加加解密数据处理中第二数据转换单元 21 中数据转换子单元的个数安排对应宽度和深度, 第二常数阵列数据的宽度为附加加解密数据处理中数据转换处理子单元的个数 M 乘以 32, 附加加解密数据处理中常数阵列数据的深度为 1;

确定附加加解密数据处理中第二常数阵列数据宽度与深度的乘积为:

附加加解密数据处理中数据转换处理子单元的个数 $M \times 32 \times 1$;

③ 附加加解密数据处理中的第二常数阵列数据应满足:

循环加解密数据处理中第一常数阵列数据宽度与深度的乘积与附加加解密数据处理中第二常数阵列数据宽度与深度的乘积 $M \times 32 \times 1$, 两者之和为 1024;

(3) 第一、第二常数阵列中相同深度的数据构成一行。

2) 将外部数据输入第二数据寄存单元 101;

(1) 将外部数据输至第二数据寄存单元 101 的输入端;

(2) 在时钟上沿或下沿, 把第二数据寄存单元 101 输入端的数据传送到其输出端。

3) 进行附加数据转换处理;

(1) 在该时钟周期内, 将第二常数阵列存储单元 301 所存储的第二常数阵列对应的数据分别输至第二数据转换单元 21 中所有的数据转换子单元 210、211 等;

(2) 在同一个时钟周期内, 第二数据寄存单元 101 输出端的数据输入到第一个数据转换子单元 210 进行数据转换处理; 第一个数据转换子单元 210 输出的数据再输入到下一个数据转换子单元 211 进行数据转换处理; 依此方式, 直至第二数据转换单元 21 中所有的数据转换子单元 210、211 等顺序完成数据转换处理, 得到第一附加加解密数据处理装置 501 的数据处理结果。

4) 以第一附加加解密数据处理装置 501 的数据处理结果作为循环加解密数据处理装置 4 中的外部数据, 用来完成循环加解密数据处理。

如图 4 所示, 为本发明实施例四在循环加解密数据处理之后增加附加加解密数据处理示意图, 包括循环加解密数据处理装置 4 和第二附加加解密数据处理装置 502。其中, 该循环加解密数据处理装置 4 的组成同上述实施例二; 该第二附加加解密数据处理装置 502 包括第三数据寄存器 102、第三常数阵列存储单元 302、以及第三数据转换单元 22, 其中该第三数据转换单元 22 包括第一数据转换子单元 220 和第二数据转换子单元 221 等。

参见图 4, 在循环加解密数据处理之后增加附加加解密数据处理的实现步骤如下:

1) 准备常数阵列;

(1) 将循环加解密数据处理所得到的第一常数阵列数据按照地址高低顺序排列, 存入第一常数阵列存储单元 3;

(2) ① 确定循环加解密数据处理中第一常数阵列的宽度和深度:

根据循环加解密数据处理中数据转换单元 2 中数据转换子单元的个数 N 安排对应宽度和深度, 得到循环加解密数据处理中第一常数阵列数据宽度与深度的乘积;

② 确定附加加解密数据处理中第三常数阵列数据的宽度和深度:

根据附加加解密数据处理中第三常数阵列数据的宽度为附加加解密数据处理中数据转换处理子单元的个数 Q 乘以 32, 附加加解密数据处理中第三常数阵列数据的深度为 1;

确定附加加解密数据处理中第三常数阵列数据宽度与深度的乘积为:

附加加解密数据处理中数据转换处理子单元的个数 $Q \times 32 \times 1$;

③ 附加加解密数据处理中的第三常数阵列数据应满足:

循环加解密数据处理中第一常数阵列数据宽度与深度的乘积与附加加解密数据处理中第三常数阵列数据宽度与深度的乘积 $Q \times 32 \times 1$, 两者之和为 1024;

(3) 常数阵列中相同深度的数据构成一行。

2) 将循环加解密数据处理装置 4 得到的数据输入第三数据寄存器 102;

(1)将循环加解密数据处理装置 4 得到的数据输至第三数据寄存单元 102 的输入端;

(2)在时钟上沿或下沿,把第三数据寄存单元 102 输入端的数据传送至其输出端。

3)进行附加数据转换处理;

(1)在该时钟周期内,将第三常数阵列存储单元 302 所存储的第三常数阵列对应的数据分别输至第三数据转换单元 22 中所有的数据转换子单元 222、221 等;

(2)在同一个时钟周期内,第三数据寄存单元 102 输出端的数据输入到第一个数据转换子单元 220 进行数据转换处理;第一个数据转换子单元 220 输出的数据再输入到下一个数据转换子单元 221 进行数据转换处理;依此方式,直至第三数据转换单元 22 中所有的数据转换子单元 220、221 等顺序完成数据转换处理,得到第二附加加解密数据处理装置 502 的数据处理结果。

4)第二附加加解密数据处理装置 502 的数据处理结果即为最终加解密数据处理结果。

附加加解密数据处理在循环加解密数据处理之前或之后进行均可,也可在之前和之后均附加该处理。参见图 5,为本发明实施例五在循环加解密数据处理之前和之后分别增加附加加解密数据处理示意图,包括:第一附加加解密数据处理装置 501、循环加解密数据处理装置 4 和第二附加加解密数据处理装置 502。其中,第一、第二附加加解密数据处理装置中的数据转换处理子单元的个数可以根据实际情况采用一个、二个或多个。

请参考图 2,本发明实施例六中:数据转换单元 2 中包括 4 个数据转换子单元,即第一数据转换子单元 200、第二数据转换子单元 201、第三数据转换子单元 202、以及第四数据转换子单元 203;第一常数阵列宽度为 128bit,深度为 8,采用循环加解密数据处理的过程进行加解密处理。实现步骤如下:

1)准备第一常数阵列;

(1)将第一常数阵列存入第一常数阵列存储单元 3;

(2)由于数据转换处理中的数据转换处理子单元为 4 个,故第一常数阵列的宽度为 128bit、深度为 8;

(3) 将宽度为 128bit 的第一常数阵列数据按深度为 8 应划分为 8 行, 每行分别命名为 rk0, rk1, ...rk7; 将每行 128bit 的第一常数阵列数据分为 4 个 32bit 的数据块, 即: rk0 分为 rk0a、rk0b、rk0c、rk0d; rk1 分为 rk1a、rk1b、rk1c、rk1d 等等。

2) 将外部数据输入第一数据寄存单元 1;

(1) 将外部数据输至第一数据寄存单元 1 的输入端。外部数据是 128bit 的数据, 分为 4 个 32bit 的数据块, 分别命名为 A0、A1、A2、A3;

(2) 在时钟上沿或下沿, 把第一数据寄存单元 1 输入端的数据传送至该第一数据寄存单元 1 的输出端, 第一数据寄存单元 1 输出 128bit 数据, 分为 4 个 32bit 的数据, 分别命名为 a0、a1、a2、a3。

3) 进行首次数据转换处理;

(1) 在该时钟周期内, 将第一常数阵列存储单元 3 所存储的第一常数阵列的第一行对应的数据分别输至所有的数据转换子单元 200 - 203;

(2) 在同一个时钟周期内, 第一数据寄存单元 1 输出端的数据输入第一个数据转换子单元 200 进行数据转换处理; 第一个数据转换子单元 200 输出的数据再输入下一个数据转换子单元 201 进行数据转换处理; 依此方式, 直至所有的数据转换子单元, 即数据转换子单元 200 - 203, 顺序完成数据转换处理。例如: 将第一数据寄存单元 1 输出端的数据 a0、a1、a2、a3 及第一常数阵列存储单元 3 输出的数据 rk0a 输送至第一个数据转换子单元 200, 转换处理后的数据仍然是 128bit, 分别命名为 B0、B1、B2、B3;

将第一个数据转换子单元 200 输出的数据 B0、B1、B2、B3 及第一常数阵列存储单元 3 输出的数据 rk0b 输送至第二个数据转换子单元 201, 转换处理后的数据仍然是 128bit, 分别命名为 C0、C1、C2、C3;

将第二个数据转换子单元 201 输出的数据 C0、C1、C2、C3 及第一常数阵列存储单元 3 输出的数据 rk0c 输送至第三个数据转换子单元 202, 转换处理后的数据仍然是 128bit, 分别命名为 D0、D1、D2、D3;

将第三个数据转换单元 202 输出的数据 D0、D1、D2、D3 及第一常数阵列存储单元 3 输出的数据 rk0d 输送至第四个数据转换单元 203, 转换处理后的数据仍然是 128bit, 分别命名为 E0、E1、E2、E3;

E0、E1、E2、E3 即是首次数据转换处理的结果数据。

4) 进行再次数据转换处理;

(1) 在时钟沿到来的时刻, 将前次数据转换处理的数据 E0、E1、E2、E3 存至第一数据寄存单元 1; 将第一数据寄存单元 1 的输出端数据 e0、e1、e2、e3 依次输入数据转换子单元 200-203;

(2) 将第一常数阵列存储单元 3 所存储的第一常数阵列的下一行对应的数据 rk1a、rk1b、rk1c、rk1d 分别输入数据转换子单元 200-203;

(3) 进行再次数据转换。

5) 重复再次数据转换处理, 得到加解密数据处理结果。

再次数据转换处理每进行一次, 即完成一个数据转换处理周期。将再次数据转换处理循环处理 6 次, 即数据转换处理共进行 8 次, 最后一次数据转换处理后输出的数据即为最终数据处理结果。

当数据转换单元 2 包括 2 个数据转换子单元时, 循环加解密数据处理共进行 16 个时钟周期完成一次加解密处理; 当数据转换单元 2 包括 8 个数据转换子单元时, 循环加解密数据处理共进行 4 个时钟周期完成一次加解密处理; 当数据转换单元 2 包括 16 个数据转换子单元时, 循环加解密数据处理共进行 2 个时钟周期完成一次加解密处理。

本发明实施例提供的实现 SMS4 密码算法中加解密处理的方法, 通过对常数阵列的安排以及对应数据转换子单元的设置, 能够减少数据转换处理的循环次数。由于单位时间内加密的数据数量大大增加, 从而提高了加密的效率。例如, 加密 128bit 的数据, 若采用 4 个数据转换子单元, 只需循环运行 8 个时钟周期就能输出最终数据处理结果。所以, 在时钟频率相同的情况下, 可以使加密效率提高 4 倍。

本发明实施例提供的实现 SMS4 密码算法中加解密处理的系统, 在满足所要求加密效率的情况下, 由于时钟频率仅为原来的 $1/n$, 故时钟频率只需原来的 $1/n$ 。例如, 加密 128bit 的数据, 若采用 4 个数据转换子单元, 时钟频率只需原来的 $1/4$ 。

此外, 在相同处理效率的情况下, 实现本发明方案的集成电路的设计、实施比较容易; 信号的完整性大大优化; 设计成本降低。此外, 采用本发明设计

集成电路，在满足所要求加密效率的情况下，由于时钟频率仅为原来的 $1/n$ ，故时钟频率只需原来的 $1/n$ 。在相同处理效率的情况下 PCB 成本降低；PCB 设计、产品易于实现；系统中的干扰降低，对其他设备、器件正常、高效工作的影响也大幅度降低。

权 利 要 求

1、一种实现 SMS4 密码算法中加解密处理的方法，其特征在于：该方法包括循环加解密数据处理的步骤，包括：

安排第一常数阵列数据的宽度和深度，相同深度的数据构成一行，存储所述第一常数阵列；

在第一时钟周期的上沿或下沿，输出寄存的外部数据；

在该第一时钟周期内，对所述存储的第一常数阵列中的第一行第一个数据，与所述寄存的外部数据进行数据转换处理，获得第一次第一转换数据；

对所述存储的第一常数阵列中的第一行第二个数据，与所述的第一次第一转换数据进行数据转换处理，获得第一次第二转换数据；

依此方式，直至将所述存储的第一常数阵列中第一行的所有数据顺序完成数据转换处理，获得第一次转换处理数据；

在第二个时钟周期的上沿或下沿到来的时刻，将第一次转换处理数据寄存起来；

在该第二时钟周期内，对所述存储的第一常数阵列中的第二行第一个数据，与所述寄存的第一次转换处理数据进行数据转换处理，获得第二次第一转换数据；

对所述存储的第一常数阵列中的第二行第二个数据，与所述的第二次第一转换数据进行数据转换处理，获得第二次第二转换数据；

依此方式，直至将所述存储的第一常数阵列中第二行的所有数据顺序完成数据转换处理，获得第二次转换处理数据；

重复上述数据转换处理过程，直至完成所有深度个数的数据转换处理过程，得到循环加解密数据处理结果。

2、根据权利要求 1 所述的实现 SMS4 密码算法中加解密处理的方法，其特征在于，所述的第一常数阵列满足以下条件：

数据按照地址由高到低的顺序排列并存储；

根据数据转换处理次数安排所述第一常数阵列数据的宽度和深度，且宽度与深度的乘积为 1024；

相同深度的数据构成一行。

3、根据权利要求 1 所述的实现 SMS4 密码算法中加解密处理的方法，其特征在于：所述的循环加解密数据处理步骤之前还包括第一附加加解密数据处理步骤，包括：

根据第一附加加解密数据处理步骤中数据转换处理的次数安排第二常数阵列数据的宽度，第二常数阵列数据的深度为 1，且相同深度的数据构成一行，存储所述第二常数阵列；

在时钟周期的上沿或下沿，输出寄存的外部数据；

在该时钟周期内，对所述存储的第二常数阵列中的第一个数据，与所述寄存的外部数据进行数据转换处理，获得第一转换数据；

对所述存储的第二常数阵列中的第二个数据，与所述的第一转换数据进行数据转换处理，获得第二转换数据；

依此方式，直至将第一附加加解密数据处理步骤中所述存储的第二常数阵列中的所有数据顺序完成数据转换处理，得到第一附加加解密数据处理结果；

以第一附加加解密数据处理结果作为循环加解密数据处理中的外部数据。

4、根据权利要求 3 所述的实现 SMS4 密码算法中加解密处理的方法，其特征在于，所述的第一常数阵列和第二常数阵列满足以下条件：

所述第二常数阵列数据宽度为第一附加加解密数据处理步骤中数据转换的次数乘以 32，所述第二常数阵列数据深度为 1，确定所述第二常数阵列数据宽度与深度的乘积；

所述第二常数阵列数据宽度与深度的乘积，与所述第一常数阵列数据宽度与深度的乘积之和为 1024。

5、根据权利要求 3 所述的实现 SMS4 密码算法中加解密处理的方法，其特征在于，所述的循环加解密数据处理步骤之后还包括第二附加加解密数据处理步骤，包括：

根据第二附加加解密数据处理步骤中数据转换次数安排第三常数阵列数据的宽度，第三常数阵列数据的深度为 1，且相同深度的数据构成一行，存储所述第三常数阵列；

将所述循环加解密数据处理结果寄存起来，在时钟周期的上沿或下沿，输出寄存的数据；

在该时钟周期内,对所述存储的第三常数阵列中的第一个数据,与所述寄存的外部数据进行数据转换处理,获得第一转换数据;

对所述存储的第三常数阵列中的第二个数据,与所述的第一转换数据进行数据转换处理,获得第二转换数据;

依此方式,直至将第二附加加解密数据处理步骤中所述存储的第三常数阵列中的所有数据顺序完成数据转换处理,得到第二附加加解密数据处理结果;所述的第二附加加解密数据处理结果即为最终加解密数据处理结果。

6、根据权利要求5所述的实现SMS4密码算法中加解密处理的方法,其特征在于,所述第一常数阵列、第二常数阵列、及第三常数阵列满足以下条件:

所述第二常数阵列数据宽度为第一附加加解密数据处理步骤中数据转换的次数乘以32,所述第二常数阵列数据深度为1,确定所述第二常数阵列数据宽度与深度的乘积;

所述第三常数阵列数据宽度为第二附加加解密数据处理步骤中数据转换的次数乘以32,所述第三常数阵列数据深度为1,确定所述第三常数阵列数据宽度与深度的乘积;

所述第二常数阵列数据宽度与深度的乘积,与所述第三常数阵列数据宽度与深度的乘积,及所述第一常数阵列数据宽度与深度的乘积之和为1024。

7、根据权利要求1所述的实现SMS4密码算法中加解密处理的方法,其特征在于,所述的循环加解密数据处理步骤之后还包括第二附加加解密数据处理步骤,包括:

根据第二附加加解密数据处理步骤中数据转换次数安排第三常数阵列数据的宽度,第三常数阵列数据的深度为1,且相同深度的数据构成一行,存储所述第三常数阵列;

将所述循环加解密数据处理结果寄存起来,在时钟周期的上沿或下沿,输出寄存的数据;

在该时钟周期内,对所述存储的第三常数阵列中的第一个数据,与所述寄存的外部数据进行数据转换处理,获得第一转换数据;

对所述存储的第三常数阵列中的第二个数据,与所述的第一转换数据进行数据转换处理,获得第二转换数据;

依此方式,直至将第二附加加解密数据处理步骤中所述存储的第三常数阵列中的所有数据顺序完成数据转换处理,得到第二附加加解密数据处理结果;所述的第二附加加解密数据处理结果即为最终加解密数据处理结果。

8、根据权利要求7所述的实现SMS4密码算法中加解密处理的方法,其特征在于,所述的第一常数阵列和第三常数阵列满足以下条件:

所述第三常数阵列数据宽度为第二附加加解密数据处理步骤中数据转换的次数乘以32,所述第三常数阵列数据深度为1,确定所述第三常数阵列数据宽度与深度的乘积;

所述第三常数阵列数据宽度与深度的乘积,与所述第一常数阵列数据宽度与深度的乘积之和为1024。

9、一种实现SMS4密码算法中加解密处理的系统,其特征在于,该系统包括循环加解密数据处理装置,所述装置包括第一常数阵列存储单元、第一数据寄存单元、以及第一数据转换单元,所述第一数据转换单元包括N个数据转换子单元;其中:

所述的第一常数阵列存储单元,用于存储第一常数阵列,以及在每一个时钟周期内,顺序的将所述第一常数阵列的每一行数据分别对应输至第一数据转换单元的N个数据转换子单元;

所述的第一数据寄存单元,用于寄存数据,以及在每一个时钟周期的上沿或下沿,将所述寄存的数据从输入端传送至输出端,并于每一个时钟周期内,将数据输至第一数据转换子单元;

所述的N个数据转换子单元,用于在每一个时钟周期内,依次进行数据转换处理,并将获得的转换数据输至下一个数据转换子单元继续处理,直至完成所有深度个数的数据转换处理过程,得到循环加解密数据处理结果。

10、根据权利要求9所述的实现SMS4密码算法中加解密处理的系统,其特征在于,所述的第一常数阵列满足以下条件:

数据的宽度和深度是根据数据转换子单元的个数N安排,且数据宽度与深度的乘积为1024,相同深度的数据构成一行,数据按照地址由高到低的顺序排列。

11、根据权利要求9所述的实现SMS4密码算法中加解密处理的系统,其

特征在于,还包括第一附加加解密数据处理装置,所述装置包括第二常数阵列存储单元、第二数据寄存单元、以及第二数据转换单元,所述第二数据转换单元包括M个数据转换子单元;其中:

所述的第二常数阵列存储单元,用于存储第二常数阵列,以及在每一个时钟周期内,顺序的将所述第二常数阵列的每一行数据分别对应输至第二数据转换单元的M个数据转换子单元;

所述的第二数据寄存单元,用于寄存数据,以及在每一个时钟周期的上沿或下沿,将所述寄存的数据从输入端传送至输出端,并于每一个时钟周期内,将数据输至第二数据转换子单元;

所述的M个数据转换子单元,用于在每一个时钟周期内,依次进行数据转换处理,并将获得的转换数据输至下一个数据转换子单元继续处理,直至完成所有深度个数的数据转换处理过程,得到第一附加加解密数据处理结果;以第一附加加解密数据处理结果作为循环加解密数据处理中的寄存数据。

12、根据权利要求11所述的实现SMS4密码算法中加解密处理的系统,其特征在于,所述的第一常数阵列和第二常数阵列满足以下条件:

该第二常数阵列数据的宽度和深度是根据第一附加加解密数据处理装置中数据转换子单元的个数M安排,且相同深度的数据构成一行;所述第二常数阵列数据宽度为第一附加加解密数据处理装置中数据转换子单元个数M乘以32,所述第二常数阵列数据深度为1,确定所述第二常数阵列数据宽度与深度的乘积为 $M \times 32 \times 1$;

所述第二常数阵列数据宽度与深度的乘积 $M \times 32 \times 1$,与所述第一常数阵列数据宽度与深度的乘积之和为1024。

13、根据权利要求11所述的实现SMS4密码算法中加解密处理的系统,其特征在于,还包括第二附加加解密数据处理装置,所述装置包括第三常数阵列存储单元、第三数据寄存单元、以及第三数据转换单元,所述第三数据转换单元包括Q个数据转换子单元;其中:

所述的第三常数阵列存储单元,用于存储第三常数阵列,以及在每一个时钟周期内,顺序的将所述第三常数阵列的每一行数据分别对应输至第三数据转换单元的Q个数据转换子单元;该第三常数阵列数据的宽度和深度是根据数

据转换子单元的个数 Q 安排的, 第三常数阵列数据的深度为 1, 且相同深度的数据构成一行;

所述的第三数据寄存单元, 用于寄存数据, 以及在每一个时钟周期的上沿或下沿, 将所述寄存的数据从输入端传送至输出端, 并于每一个时钟周期内, 将数据输至第三数据转换子单元;

所述的 Q 个数据转换子单元, 用于在每一个时钟周期内, 依次进行数据转换处理, 并将获得的转换数据输至下一个数据转换子单元继续处理, 直至完成所有深度个数的数据转换处理过程, 得到第二附加加解密数据处理结果; 所述的第二附加加解密数据处理结果即为最终加解密数据处理结果。

14、根据权利要求 13 所述的实现 SMS4 密码算法中加解密处理的系统, 其特征在于, 所述第一常数阵列、第二常数阵列、及第三常数阵列满足以下条件:

所述第二常数阵列数据的宽度和深度是根据第一附加加解密数据处理装置中数据转换子单元的个数 M 安排, 且相同深度的数据构成一行; 该第二常数阵列数据宽度为第一附加加解密数据处理装置中数据转换子单元个数 M 乘以 32, 所述第二常数阵列数据深度为 1, 确定所述第二常数阵列数据宽度与深度的乘积为 $M \times 32 \times 1$;

所述第三常数阵列数据的宽度和深度是根据第二附加加解密数据处理装置中的数据转换子单元的个数 Q 安排, 且相同深度的数据构成一行; 该第三常数阵列数据宽度为第二附加加解密数据处理装置中数据转换子单元个数 Q 乘以 32, 所述第三常数阵列数据深度为 1, 确定所述第三常数阵列数据宽度与深度的乘积为 $Q \times 32 \times 1$;

所述第二常数阵列数据宽度与深度的乘积 $M \times 32 \times 1$, 与所述第三常数阵列数据宽度与深度的乘积 $Q \times 32 \times 1$, 及所述第一常数阵列数据宽度与深度的乘积之和为 1024。

15、根据权利要求 9 所述的实现 SMS4 密码算法中加解密处理的系统, 其特征在于, 还包括第二附加加解密数据处理装置, 所述装置包括第三常数阵列存储单元、第三数据寄存单元、以及第三数据转换单元, 所述第三数据转换单元包括 Q 个数据转换子单元; 其中:

所述的第三常数阵列存储单元,用于存储第三常数阵列,以及在每一个时钟周期内,顺序的将所述第三常数阵列的每一行数据分别对应输至第三数据转换单元的Q个数据转换子单元;

所述的第三数据寄存单元,用于寄存数据,以及在每一个时钟周期的上沿或下沿,将所述寄存的数据从输入端传送至输出端,并于每一个时钟周期内,将数据输至第三数据转换子单元;

所述的Q个数据转换子单元,用于在每一个时钟周期内,依次进行数据转换处理,并将获得的转换数据输至下一个数据转换子单元继续处理,直至完成所有深度个数的数据转换处理过程,得到第二附加加解密数据处理结果;所述的第二附加加解密数据处理结果即为最终加解密数据处理结果。

16、根据权利要求15所述的实现SMS4密码算法中加解密处理的系统,其特征在于,所述的第一常数阵列和第三常数阵列满足以下条件:

所述第三常数阵列数据的宽度和深度是根据第二附加加解密数据处理装置中的数据转换子单元的个数Q安排,且相同深度的数据构成一行;该第三常数阵列数据宽度为第二附加加解密数据处理装置中数据转换子单元个数Q乘以32,所述第三常数阵列数据深度为1,确定所述第三常数阵列数据宽度与深度的乘积为 $Q \times 32 \times 1$;

所述第三常数阵列数据宽度与深度的乘积 $Q \times 32 \times 1$,与所述第一常数阵列数据宽度与深度的乘积之和为1024。

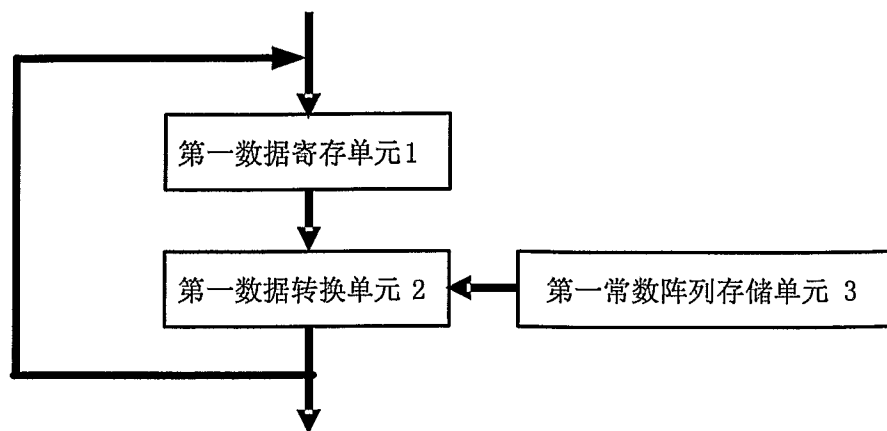


图 1

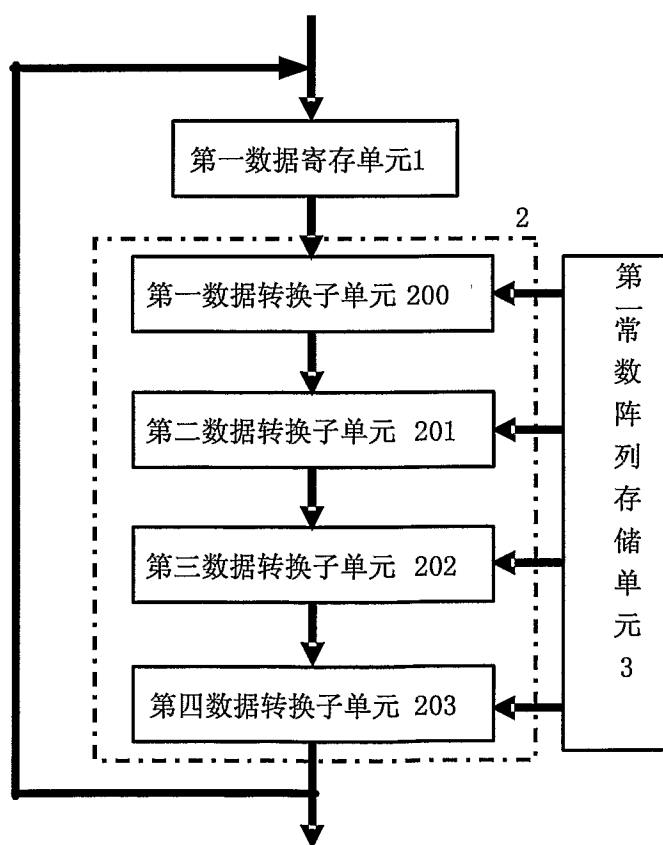


图 2

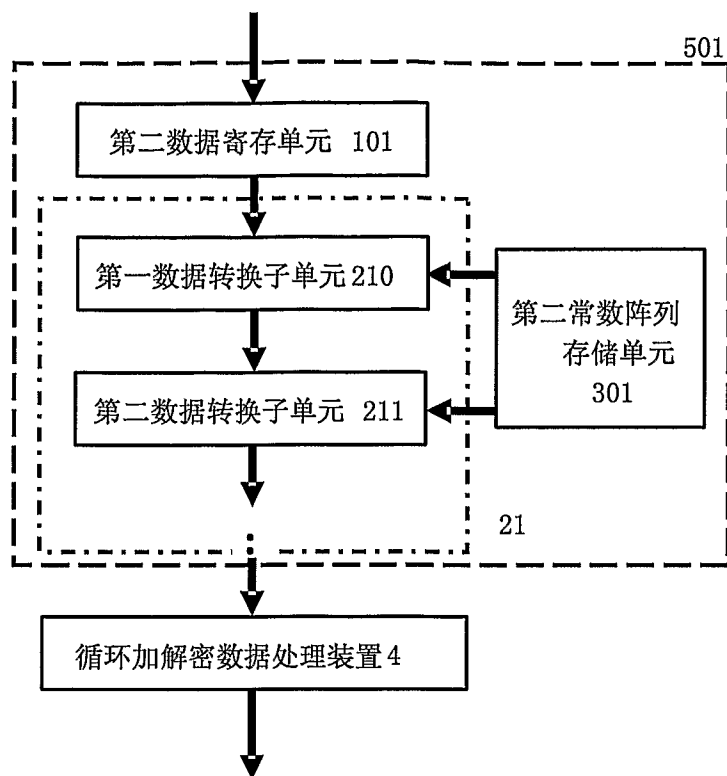


图 3

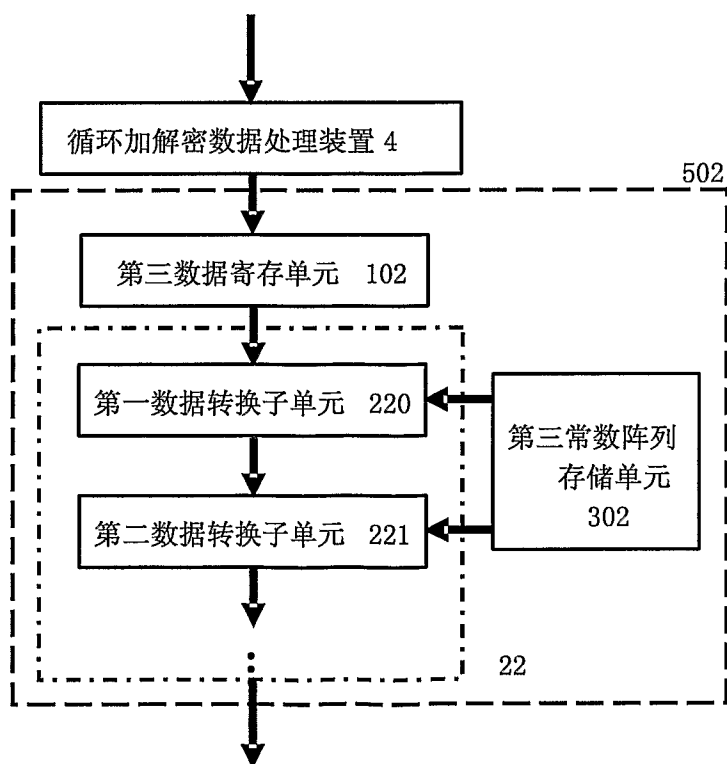


图 4

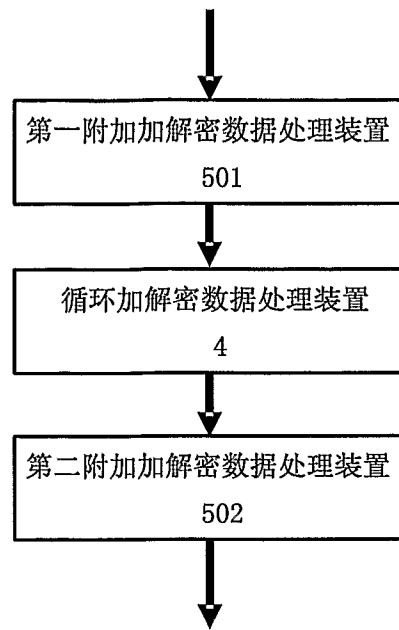


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2007/000617

A. CLASSIFICATION OF SUBJECT MATTER

See the extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06F12/16,G06F12/14,G06F12/00,H04L9/28,H04L9/14,H04L9/00,G06F17/00,G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI,EPODOC,PAJ,CNPAT: SMS,??cipher+,??cod+,password,??crypt+,data,datum,process+,stor+,memor+,constant, convers+,short,message,service,deposit+,const,persistenc?,depth,depth,width,breadth,load+,register

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN1610291A (MINGHUA AUHAN SCI & TECHNOLOGY CO LTD SHENZHEN CITY) 27 Apr. 2005 (27.04.2005) the whole document	1-16
A	WO03096615A1 (WIRELESS APPLICATIONS PTY LTD) 20 Nov. 2003 (20.11.2003) the whole document	1-16
A	US20040224704A1 (M.Khaledul ISLAM et al.) 11 Nov. 2004 (11.11.2004) the whole document	1-16

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 24 May 2007 (24.05.2007)	Date of mailing of the international search report 07 Jun. 2007 (07.06.2007)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer XU Yan Telephone No. (86-10) 62085794

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2007/000617

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1610291A	27.04.2005	none	
WO03096615A1	20.11.2003	US2006098678 A1	11.05.2006
		EP1502383 A1	02.02.2005
		CN1653746 A	10.08.2005
		AU2003225327A1	11.11.2003
US2004224704 A1	11.11.2004	US2006211434 A1	21.09.2006
		WO2004056138A2	01.07.2004
		AU2003294522A1	09.07.2004
		EP1570690A2	07.09.2005
		BRPI0316604A	11.10.2005
		MXPA05006344A	01.09.2005
		JP2006510278T	23.03.2006
		KR20050085643A	29.08.2005
		CN1745593A	08.03.2006
		US2006211434A1	21.09.2006

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2007/000617

IPC CLASSIFICATION:

G09C1/00 (2006.01) i

G06F12/16 (2006.01) i

H04L9/28 (2006.01) i

国际检索报告

国际申请号
PCT/CN2007/000617

A. 主题的分类

参见附加页

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: G06F12/16,G06F12/14,G06F12/00,H04L9/28,H04L9/14,H04L9/00,G06F17/00,G09C1/00

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

WPI,EPODOC,PAJ,CNPAT: 密码, 加密, 解密, 加解密, 数据, 短信服务, 存储, 寄存, 储存, 贮存, 常数, 常值, 恒定值, 恒值, 深度, 宽度, SMS,??cipher+,??cod+,password,??crypt+,data,datum,process+,stor+,memor+,constant, convers+,short,message,service,deposit+,const,persistenc?,depth,depth,width,breadth,load+,register

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	CN1610291A (深圳市明华澳汉科技股份有限公司) 27.4 月 2005 (27.04.2005) 全文	1-16
A	WO03096615A1 (WIRELESS APPLICATOINS PTY LTD) 20.11 月 2003 (20.11.2003) 全文	1-16
A	US20040224704A1 (M.Khaledul ISLAM 等) 11.11 月 2004 (11.11.2004) 全文	1-16

☐ 其余文件在 C 栏的续页中列出。

☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

24.5 月 2007 (24.05.2007)

国际检索报告邮寄日期

07.6 月 2007 (07.06.2007)

中华人民共和国国家知识产权局(ISA/CN)

中国北京市海淀区蓟门桥西土城路 6 号 100088

传真号: (86-10)62019451

受权官员

许彦

电话号码: (86-10) 62085794

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2007/000617

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN1610291A	27.04.2005	无	
WO03096615A1	20.11.2003	US2006098678 A1	11.05.2006
		EP1502383 A1	02.02.2005
		CN1653746 A	10.08.2005
		AU2003225327A1	11.11.2003
US2004224704 A1	11.11.2004	US2006211434 A1	21.09.2006
		WO2004056138A2	01.07.2004
		AU2003294522A1	09.07.2004
		EP1570690A2	07.09.2005
		BRPI0316604A	11.10.2005
		MXPA05006344A	01.09.2005
		JP2006510278T	23.03.2006
		KR20050085643A	29.08.2005
		CN1745593A	08.03.2006
		US2006211434A1	21.09.2006

国际 IPC 分类:

G09C1/00 (2006.01) i

G06F12/16 (2006.01) i

H04L9/28 (2006.01) i