基于可编程逻辑器件的单向壳核函数构造方法

李 蕴 奇
(吉林省经济信息中心, 长春 130061)

摘要: 针对构造公钥密码时出现函数单向性和陷门性矛盾的问题, 通过引入单向壳核函数新型公钥密码体制, 根据可编程逻辑器件PLD的设计思想和结构特征, 给出一种单向壳核函数的构造方法, 其安全性等同于一次一密. 与传统公钥密码体制相比, 单向壳核函数具有更广的包容性和更高的安全性, 是一种灵活性更强的公钥密码体制.

关键词: 公钥密码; 单向壳核函数; 可编程逻辑器件
中图分类号: TP309 **文献标志码**: A **文章编号**: 1671-5489(2012)02-0305-04

Construction Method of One-Way Shell Core Function Based on Programmable Logic Device

LI Yun-qi
(*Center of Economic and Information in Jilin Province*, *Changchun* 130061, *China*)

Abstract: In view of the contradiction between one way and trapdoor occured on constructing public key cryptography, the author introduced a new type of public key cryptography that is one-way shell core function. According to the designing ideas and structural characteristics of programmable logic device (PLD), the paper presents a scheme of one-way shell core function and shows that its security is equal to that of one-time pad. Compared with the traditional public key cryptography, one-way shell core function has the characteristics of wider inclusivity, more change and higher security. The function provides people with a public key cryptography of more flexibility.

Key words: public key cryptography; one-way shell core function; programmable logic device

近年来, 信息安全领域越来越受到人们的广泛关注, 而公钥密码是信息安全的核心和主干. 因此, 构造一种安全可靠的公钥密码体制成为人们的研究热点. 传统公钥密码构造的关键是找到合适的单向函数或单向陷门函数. 在选取单向函数、构造公钥密码的过程中, 找到单向函数较容易, 但找到满足交换性的单向函数族非常困难. 同理, 在选取单向陷门函数、构造公钥密码的过程中, 为便于解密, 就要设计一个合适的陷门, 而增加了陷门就会牺牲函数的单向性, 留下安全隐患, 因此, 要构造出安全性较高的单向陷门函数, 必须平衡单向性和陷门性二者的矛盾[1-5]. 本文引入一种新的公钥密码体制, 即单向壳核函数. 这种密码体制更灵活、安全, 且无需满足交换性.

1 单向壳核函数

根据单向函数的定义, 对于已知 x, 易计算出 $y=f(x)$, 而对于已知 y, 若计算 x 使得 $y=f(x)$ 很困难. 因此, 单向函数相当于将已知 x 封闭在盒子中, 如图1所示.

根据单向陷门函数的定义, 对于已知 x, 易计算出 $y=f(x)$, 而对于已知 y, 若计算 x 使得 $y=f(x)$

收稿日期: 2011-03-19.
作者简介: 李蕴奇(1976—), 女, 汉族, 硕士, 工程师, 从事信号处理和分布式数据库应用的研究, E-mail: li__yunqi@sina.com.
基金项目: 国家自然科学基金(批准号: 40972059).

很困难，但如果获知了陷门 k，要计算 x 使得 $y=f(x)$ 则较容易. 因此，单向陷门函数相当于把已知 x 封闭在带有开关的盒子中，结构如图2所示.

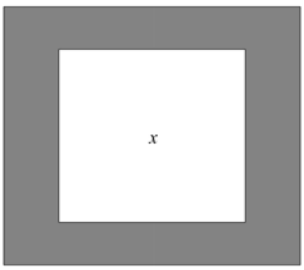

图1 单向函数

Fig. 1 One-way function

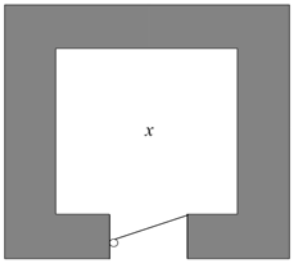

图2 单向陷门函数

Fig. 2 One-way trapdoor function

根据单向函数和单向陷门函数的特点，本文给出一种更灵活的新型函数——单向壳核函数，结构如图3所示.

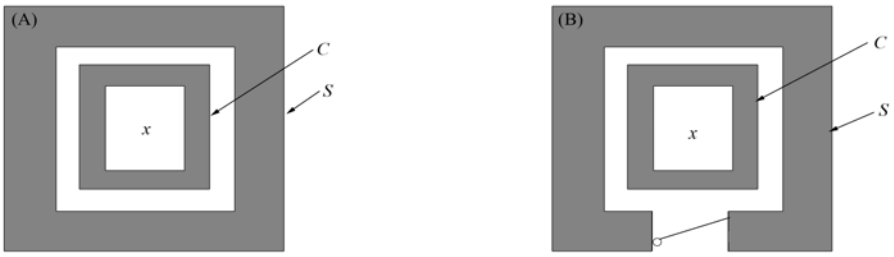

图3 单向壳核函数

Fig. 3 One-way shell core function

由图3可见，本文引入了核函数 C 和壳函数 S，并引入了函数 S 和 C 的逆变换，即剥壳函数 S^{-1} 和剥核函数 C^{-1}（剥核函数 C^{-1} 基本不用）. $SC(x)=S\circ C(x)=S(C(x))$，即壳核函数 $SC(x)$ 为核函数 C 和壳函数 S 的复合运算[6-7].

2 单向壳核函数的构造

2.1 可编程逻辑器件 PLD

可编程逻辑器件 PLD 是面向特定用途集成电路 ASIC 的重要组成部分. 可编程逻辑器件具有很强的灵活性. 用户可根据自己的需求编写程序，构建出新的功能，进而得到功能强大的芯片. 与-或阵列都是可编程逻辑器件的主体，虽然输入相似，但输出差异较大[8-10].

熔丝式编程单元是一种典型的 PLD 编程单元，如图4所示. 熔丝式编程单元由一个双极型晶体管 T 与连接在晶体管发射极的一条熔丝组成. 当通过熔丝的电流达到一定值时，熔丝就会烧断. 利用电流是否烧断相应行列交汇处熔丝这一原理进行编程，当熔丝未被烧断，则输出为“1”；相反，当熔丝烧断，则输出为“0”.

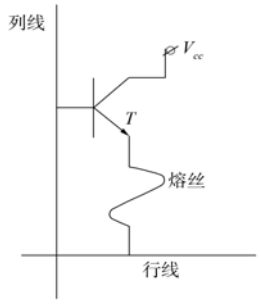

图4 熔丝式编程单元

Fig. 4 Programmable unit based on the type of fuse wires

根据熔丝式编程单元的特点，人们开发了基于熔丝式编程单元或阵列的芯片，如图5所示. 相对于与阵列的固定性，或阵列具有更大的灵活性，用户可根据自己的需要，编写适当的程序.

2.2 基于可编程逻辑器件 PLD 的构造方法

基于可编程逻辑器件 PLD 的思想构造单向壳核函数的第一种结构(图3(A))，即壳函数 S 与核

函数 C 皆为单向函数. 基于 PLD 思想构造的单向壳核函数原理如图 6 所示. 分别选取核函数 $C(x)=\mathrm{PLD}_1(x_1,x_2,\cdots,x_n)$ 和壳函数 $S(x)=\mathrm{PLD}_2(x_1,x_2,\cdots,x_{n_1})$，其中 PLD_1 与 PLD_2 分别具有不同的输入个数. 工作原理如下：

1）随机烧断 PLD_1 与 PLD_2 或阵列中的熔丝. 其中，PLD 中每个输出都是输入的逻辑函数，可根据需要任意选取逻辑函数.

2）在明文通过复合的逻辑器件组前，先将明文 x 表示为$(x_1,x_2,\cdots,x_n)$，再将其输入.

3）当输入的$(x_1,x_2,\cdots,x_n)$，经过第一个逻辑器件 $C(x)=\mathrm{PLD}_1(x_1,x_2,\cdots,x_n)$操作后，获得 n_1 个输出结果，即$(F_1',F_2',\cdots,F_{n_1}')$. 其中输入个数 n 与输出个数 n_1 应满足相近条件. 因为如果有 2^n-1 个输出，则当 n 足够大时，必然会使芯片成本增加，产生不必要的资源浪费.

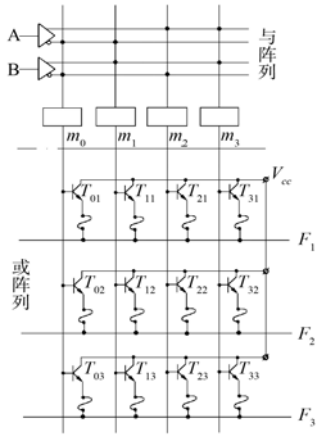

图 5　熔丝式编程单元结构

Fig. 5　Structure of programmable units based on the type of fuse wires

4）将获得的中间结果$(F_1',F_2',\cdots,F_{n_1}')$作为第二个逻辑器件 $S(x)=\mathrm{PLD}_2(x_1,x_2,\cdots,x_{n_1})$的输入，会获得 n_2 个输出结果，即获得了最终结果$(F_1,F_2,\cdots,F_{n_2})$. 同理，输入个数 n_1 与输出个数 n_2 应该相近.

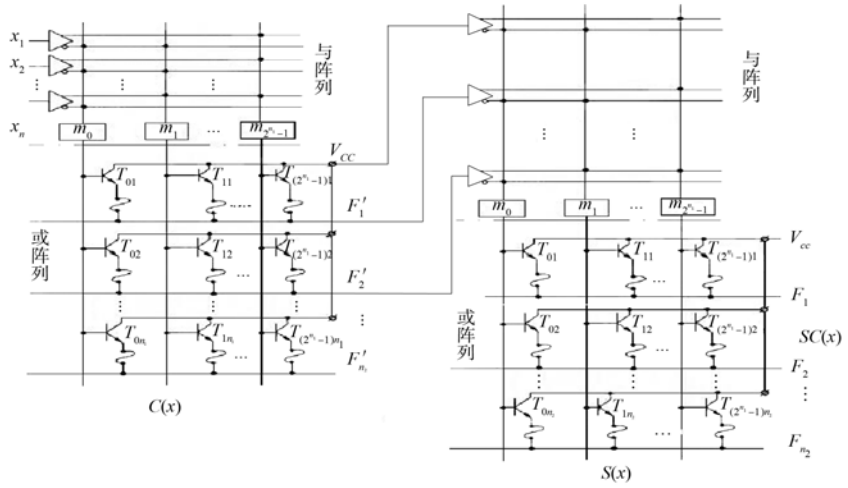

图 6　基于 PLD 的单向壳核函数

Fig. 6　One-way shell core function based on PLD

2.3　安全分析

从基于 PLD 思想的单向壳核函数原理可见，该函数的安全性主要依赖于“黑箱”函数的安全性. “黑箱”函数的操作过程相当于一次一密过程. 每次对敏感信息加密都随机生成不相同的密钥，即密钥使用一次后就不重复使用. 若再次加密一个新的明文信息，则必须重新生成一个新密钥. 如果攻击者采用穷举攻击的方法进行破解，会尝试多种可能的密钥，由此得到多个明文信息，但无法确定哪个明文是有价值的，因为得到的明文信息与随机输出间无任何统计关系. 输出得到的密文信息中不包含任何有关明文的信息，因此一次一密目前被认为是安全的，无法攻破的. 如果密钥中的字符流都具有真随机性，则输出得到的字符流也是真随机的，攻击者更难破解.

基于 PLD 思想构造的单向壳核函数中，或阵列构成的“黑箱”函数起关键作用. 其中的每个输出都是输入的逻辑函数，可随机选取具体的“黑箱”函数. “黑箱”函数的任意选取确保了密钥交换过程的安

全性. 如果函数的输入和输出间有明确的表达式, 则函数易受到插值攻击. 图6中, 核函数 $C(x)$ 对应的 PLD_1 与壳函数 $S(x)$ 对应的 PLD_2 组成复合芯片, 在两个或阵列中的任一熔丝均可根据需要被随机烧断. 通信双方在每次进行密钥交换前, 都要先通过随机烧断不同熔丝构造不同的阵列组合. 阵列组合确定后, 通信双方即利用烧好的PLD器件完成密钥交换. 按照该方法进行操作, 不同明文输入进入随机烧断不同熔丝阵列的变换, 等同于一次一密的变换过程, 随机性较强, 不可攻破. 每次先将 n 个输入经过 PLD_1 变换, 即经过核函数 $C(x)$ 的变换操作, 将获得 n_1 个输出的中间结果. 再把得到的 n_1 个中间结果输入到 PLD_2, 即经过壳函数的变换 $S(x)$ 操作, 得到 n_2 个输出结果, 输出的 n_2 个结果即为单向壳核函数 $SC(x)$ 的值. 壳函数 $S(x)$ 与核函数 $C(x)$ 都是不可逆的单向函数, 其中的输入个数 n 应与中间输出个数 n_1 及最终输出个数 n_2 相近.

综上所述, 本文通过引入单向壳核函数公钥密码体制, 根据可编程逻辑器件PLD的设计思想, 构造了单向壳核函数, 并进行了安全性分析, 证明了这种新型的公钥密码具有较强的安全性.

参 考 文 献

[1] William Stallings. 密码编码学与网络安全原理与实践 [M]. 杨明, 译. 北京: 电子工业出版社, 2001.

[2] 曹珍富. 公钥密码学 [M]. 哈尔滨: 黑龙江教育出版社, 1993.

[3] SHI Zheng-xi, ZHANG Jun-hua. The Current Study on and Developing Trends of the Information Security Home and Abroad [J]. Sci-Tech Information Development & Economy, 2007, 17(10): 97-98. (石正喜, 张君华. 国内外信息安全研究现状及发展趋势 [J]. 科技情报开发与经济, 2007, 17(10): 97-98.)

[4] YUAN Zhe, ZHAO Yong-zhe, ZHANG Wen-rui, et al. Secure Transfer of Sensitive Data [J]. Journal of Jilin Teachers Institute of Engineering and Technology, 2008, 24(1): 73-77. (袁哲, 赵永哲, 张文睿, 等. 敏感数据安全传输方法 [J]. 吉林工程技术师范学院学报, 2008, 24(1): 73-77.)

[5] YUAN Zhe, ZHAO Yong-zhe, LI Guang-wei, et al. Implement of Key-Exchange Based on the Hidden-Bases via Ergodic Matrix over Finite Field [J]. Journal of Jilin University: Science Edition, 2009, 47(4): 783-789. (袁哲, 赵永哲, 李光伟, 等. 利用有限域上遍历矩阵实现基于隐藏基的密钥交换 [J]. 吉林大学学报: 理学版, 2009, 47(4): 783-789.)

[6] SUN Yan-jun, YUAN Zhe. Application of One-Way Shell Core Function in Cryptography [J]. Computer Knowledge and Technology, 2010, 6(11): 2791-2793. (孙延君, 袁哲. 单向壳核函数在密码学中的应用 [J]. 电脑知识与技术, 2010, 6(11): 2791-2793.)

[7] SUN Yan-jun, ZHANG Yan, YUAN Zhe. The Public Key Cryptography Base on One-Way Shell Core Function [J]. Computer Knowledge and Technology, 2010, 6(15): 4321-4323. (孙延君, 张岩, 袁哲. 基于单向壳核函数的公钥密码 [J]. 电脑知识与技术, 2010, 6(15): 4321-4323.)

[8] 毛法尧. 数据逻辑 [M]. 北京: 高等教育出版社, 2000.

[9] 王玉龙. 数字逻辑实用教程 [M]. 北京: 清华大学出版社, 2002.

[10] 郑川, 张卫军. Step By Step 现场可编程门阵列设计入门与进阶 [M]. 西安: 西安电子科技大学出版社, 2008.

(责任编辑: 韩 啸)