

快速 CRC 逆序校验方法

梁海华*, 盘丽娜

(常熟理工学院 计算机科学与工程学院, 江苏 常熟 215500)

(* 通信作者电子邮箱 edward_3me@163.com)

摘要:循环冗余校验(CRC)是计算机网络中常用的冗余校验方法。针对现有的正序(FIFO)校验方法只能对编码寄存器为零初始状态时生成的校验值正确校验的问题,提出一种逆序(LIFO)校验方法。首先,使用状态矩阵对两类串行编码电路进行分析,理论上证明状态矩阵可逆,由逆矩阵变换得出串行逆序校验方法及其电路;通过电路分析,可将串行逆序方法扩展为快速并行逆序方法,无须预补零操作,简化了计算流程。通过实例计算,验证了并行逆序方法能够对任意初始状态生成的校验值正确校验;仿真结果表明该方法具有与并行正序校验方法近似的运算速度。

关键词:循环冗余校验;先进先出;初始状态;后进先出;运算速度

中图分类号:TP393 **文献标志码:**A

Method of fast cyclic redundancy check reverse decoding

LIANG Haihua*, PAN Lina

(School of Computer Science and Engineering, Changshu Institute of Technology, Changshu Jiangsu 215500, China)

Abstract: Cyclic Redundancy Check (CRC) has already been used in the field of computer network widely. Since the existing First In First Out (FIFO) method can only decode checksum which is encoded when initial register's state is zero, a Last In First Out (LIFO) method was proposed. First of all, by analyzing two kinds of serial encoding circuit based on transition of state matrix, the authors theoretically proved the matrix was invertible, and serial LIFO method and its circuit could be derived. Depending on serial method, rapid parallel LIFO method was given, in no need of dummy bits, thus simplifying the calculation process. A case study verified the correctness of this method when decoding checksum, no matter what initial register's state was. The simulation results show that FIFO and LIFO have similar calculation speed.

Key words: Cyclic Redundancy Check (CRC); First In First Out (FIFO); initial state; Last In First Out (LIFO); calculation speed

0 引言

目前,在计算机通信领域,由于数据在传输或存储过程中会受到各种干扰产生误码,从而需要进行数据校验来确保数据的完整性,循环冗余校验(Cyclic Redundancy Check, CRC)是一种常用的方法^[1-2],Peterson等提出了两种串行编码电路^[3],Giuseppe等^[4]和Cheng等^[5]分别从不同的角度提出了并行编码方式;为了破解软件中CRC校验值的保护,Stigge等从串行编码计算方法角度提出了一种按位进行的CRC逆向求解方法^[6]。本文从编码电路状态分析入手提出一种并行的快速CRC逆序校验方法;解决现有CRC校验方法只能判定编码电路零初始状态时生成的校验值是否正确的问题;解决现有方法中需预先填零操作,使得处理数据长度是并行处理位宽整数倍的问题^[7],提高处理的实时性。

CRC一般编码及校验方法:发送信息序列 $b_0b_1\cdots b_{n-1}b_n$ 对应多项式为 $M(X) = b_0X^n + b_1X^{n-1} + \cdots + b_{n-1}X + b_n$,生成多项式 $G(X) = p_mX^m + p_{m-1}X^{m-1} + \cdots + p_1X + p_0$,校验序列 $R(X) = M(X) \times X^m \bmod G(X)$ 对应多项式为 $R(X) = r_{m-1}X^{m-1} + r_{m-2}X^{m-2} + \cdots + r_1X + r_0$,发送序列 $M_s(X) = M(X) \times X^m + R(X)$;接收序列 $M_r(X)$,如果无差错接收 $M_r(X) = M_s(X)$,则 $M_r(X) \bmod G(X) = 0$,否则出错。图1为现有 m 级串行CRC编码器的结构示意图,寄存器初始状态一般情况下为零(即零初态);图2为现有 m 级串行CRC

解码器结构示意图,解码器为零初态。

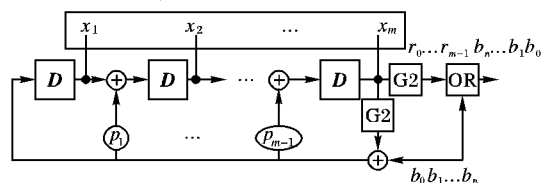


图1 $p_mX^m + p_{m-1}X^{m-1} + \cdots + p_1X^1 + p_0 (p_0 = 1, p_m = 1)$ 对应串行编码电路

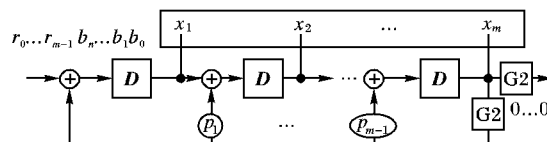


图2 $p_mX^m + p_{m-1}X^{m-1} + \cdots + p_1X^1 + p_0 (p_0 = 1, p_m = 1)$ 对应的FIFO串行解码电路

现行CRC解码器基本都是基于该原理实现的,采用该结构的CRC解码器是一种先进先出(First In First Out, FIFO)的正序处理方式;该解码器可以实现零初态的校验,但无法完成非零初态CRC编码的信道差错判定工作(具体见实验)。

1 串行CRC逆序解码

首先给出假设,生成多项式的最高次幂是 m (长度为 $m+1$), $(p_0, p_1, \cdots, p_{m-1}, 1)$ 为生成多项式的低次项到高次项的系

数,校验序列长度为 m ,并行处理长度为 w , $x_i(1 \leq i \leq m)$ 为寄存器 i 的状态,输入的处理数据为 $b_0 b_1 \cdots b_n$ 。

文献[8]中提出了常用的系统分析方法——状态矩阵分析法,由文献[4]可知如下结论:

图1的状态方程为 $X' = F^w \otimes (X \oplus D)$ (此处 \otimes 为异或、与构成的矩阵操作), $X = (x_m, \cdots, x_2, x_1)^T$ 表示系统的初始状态(零时刻), $D = [b_0 \cdots b_{w-1} | 0 \cdots 0]^T$ 为 w 位输入, X' 表示 w 时刻的系统状态($w \leq m$)。 $X' = F^w \otimes (X \oplus D)$ 可以改写为 $X' = (F^w \otimes X) \oplus (F^w \otimes D)$,若为零初态即 $X = 0$,则 $X' = F^w \otimes D$,非零初态相当于给输出的校验码 X' 添加了伪随机序列 $F^w \otimes X$,捎带增强了CRC的安全性^[9-11]。

图2存在类似结果 $X' = F^w \otimes X \oplus D$, $D = [0 \cdots 0 | b_0 \cdots b_{w-1}]^T$, $X = (x_m, \cdots, x_2, x_1)^T$ 。其中:

$$F = \begin{bmatrix} p_{m-1} & 1 & 0 & \cdots & 0 \\ p_{m-2} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_1 & 0 & 0 & \cdots & 1 \\ p_0 & 0 & 0 & \cdots & 0 \end{bmatrix}; w \leq m$$

文献[12]将上述状态方程扩展到 $w > m$ 条件下。

令 $x_i(t)(1 \leq i \leq m)$ 为寄存器 i 的 t 时刻状态,对图1进行状态分析可得:

$$\begin{bmatrix} x_m(t+1) \\ x_{m-1}(t+1) \\ \vdots \\ x_2(t+1) \\ x_1(t+1) \end{bmatrix} = \begin{bmatrix} p_{m-1} & 1 & 0 & \cdots & 0 \\ p_{m-2} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_1 & 0 & 0 & \cdots & 1 \\ p_0 & 0 & 0 & \cdots & 0 \end{bmatrix} \otimes \begin{bmatrix} x_m(t) \\ x_{m-1}(t) \\ \vdots \\ x_2(t) \\ x_1(t) \end{bmatrix} \oplus \begin{bmatrix} b(t) \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix}$$

令

$$F = \begin{bmatrix} p_{m-1} & 1 & 0 & \cdots & 0 \\ p_{m-2} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_1 & 0 & 0 & \cdots & 1 \\ p_0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

公式可简写为:

$$X(t+1) = F \otimes X(t) \oplus \begin{bmatrix} b(t) \\ \vdots \\ 0 \\ 0 \end{bmatrix} \quad (1)$$

通过计算可得行列式 $\det(F) = p_0 = 1 \neq 0$, F 存在逆矩阵 F^{-1} ,通过初等列变换得:

$$F^{-1} = \begin{bmatrix} 0 & \cdots & 0 & 0 & 1 \\ 1 & \cdots & 0 & 0 & p_{m-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 & p_2 \\ 0 & \cdots & 0 & 1 & p_1 \end{bmatrix}$$

因此可由式(1)推导得:

$$X(t) = F^{-1} \otimes X(t+1) \oplus \begin{bmatrix} b(t) \\ \vdots \\ 0 \\ 0 \end{bmatrix}$$

令

$$\Gamma = \begin{bmatrix} p_1 & 1 & 0 & \cdots & 0 \\ p_2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{m-1} & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

式子可变换为:

$$\begin{bmatrix} x_1(t) \\ x_2(t) \\ \vdots \\ x_{m-1}(t) \\ x_m(t) \end{bmatrix} = \begin{bmatrix} p_1 & 1 & 0 & \cdots & 0 \\ p_2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{m-1} & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix} \otimes \begin{bmatrix} x_1(t+1) \\ x_2(t+1) \\ \vdots \\ x_{m-1}(t+1) \\ x_m(t+1) \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ b(t) \end{bmatrix}$$

简写为:

$$X'(t) = \Gamma \otimes X'(t+1) \oplus \begin{bmatrix} 0 \\ \vdots \\ 0 \\ b(t) \end{bmatrix} \quad (2)$$

式(1)中 $X(t)$ 为CRC编码寄存器 t 时刻的状态, $X(t+1)$ 为CRC编码电路由一位信息比特 $b(t)$ 生成的校验序列;通过式(2), $X'(t+1)$ 为 $X(t+1)$ 的逆序,由 $X'(t+1)$ 、 $b(t)$ 计算得 $X'(t)$,若 $X'(t)$ 的逆序与编码时的状态 $X(t)$ 一致,说明传输过程中无错误,否则有错误发生。对应的后进先出(Last In First Out, LIFO)的逆序串行解码电路(解码器为零初态)如图3所示,要求输入序列与状态序列都逆序,最后得到系统初态 $X'(t)$ 也是逆序的,据此可判断传输过程是否有错误发生。

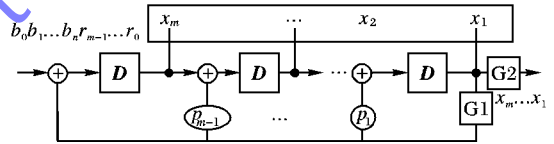


图3 $p_m X^m + p_{m-1} X^{m-1} + \cdots + p_1 X^1 + p_0 (p_0 = 1, p_m = 1)$ 对应的LIFO串行解码电路

2 并行CRC逆序校验

由上分析可得一种串行的CRC逆序校验算法,该算法能够对任意初态的CRC编码进行校验。

根据状态矩阵 F 的特性可获得 P 矩阵(图4)。为了提高CRC校验的运算速度,满足高速链路的要求,根据第1章电路分析及文献[12]的扩展,串行方法可拓展为并行处理的快速CRC逆序校验方法,与文献[7]中的并行CRC正序校验(FIFO)处理流程相比,无须通过预补零操作使得输入处理数据位是并行处理位宽的整数倍,精简了计算流程,如下所示(CRC逆序校验算法)。

将 $M_R(X)$ 序列(若为无差错接收,其逆序为 $(r_0 \cdots r_{m-1} b_n \cdots b_0)$,长度为 $l = m + n + 1, l > m$)的逆序 $(a_1 \cdots a_l)$,生成多项式 $G(X)$ 的最高次幂 m 、并行处理带宽 w 代入CRC逆序校验算法即可获得CRC编码器的初始状态。

CRC逆序校验算法 $R = \text{crc}^{-1}(m, w, P_w, a_1 \cdots a_l), \lfloor x \rfloor$ 表示比 x 小的最大整数。

输入: 输入比特流 $(a_1 \cdots a_l)$, 长度为 l , 并行带宽 w , 寄存器数 m 。

$L = l - m$;

$k = \lfloor L/w \rfloor$;

for $i = 0$ to $k - 1$ do

$$R = P_w \otimes (a_{i+w+1} \cdots a_{(i+1)*w})^T;$$

$$(a_{(i+1)*w+1} \cdots a_{(i+1)*w+m}) = (a_{(i+1)*w+1} \cdots a_{(i+1)*w+m}) \oplus R^T;$$

$$L = L - w;$$

end for

if $L \neq 0$ then

$$R = P_L \otimes (a_{k+w+1} \cdots a_{k+w+L})^T$$

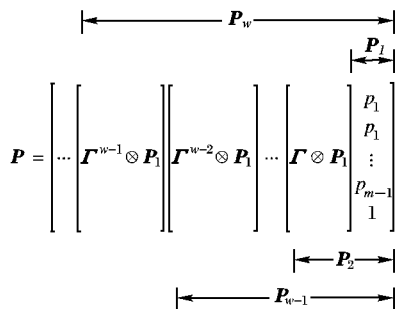
$$(a_{l-m+1} \cdots a_l) = (a_{l-m+1} \cdots a_l) \oplus R^T$$

end if

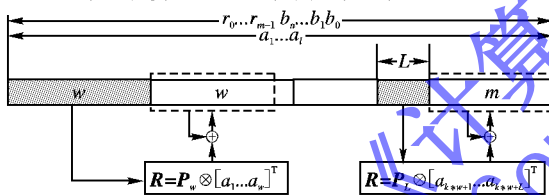
$$R = (a_{l-m+1} \cdots a_l)$$

输出: $R = (X_1 \cdots X_m)$ (m 个寄存器的最终状态)。

注:由于 P_L 中 $L < w$, 由图4可知 P_L 包含在 P_w 中, 无须重新生成。

图4 查询矩阵 P

CRC 逆序校验算法通过分组实现, 且并行位宽需满足 $1 \leq w \leq l - m$ 。当 $w = 1$ 为图3中的串行方案; 当 $w > m$ 时, 如图5所示, 当 $w \leq m$ 时, 处理过程与图5类似; 当 $w = l - m$ 时, CRC 逆序校验算法可以一次解码完成。

图5 $w > m$ 时, 分组CRC逆序校验算法

最后, $R = (X_1 \cdots X_m)$ 与图1中CRC编码器的寄存器初态 $(X_m \cdots X_1)$ 的逆序比较, 如果序列相等接收正确, 否则发生错误; 特别对于零初态CRC编码, 本解码器与正序解码方法类似, 也只需判断 R 是否为全零, 若是, CRC 校验正确; 否则校验错误, 接收序列有错误发生。

3 实验与分析

以宽带码分多址/时分同步码分多址/长期演进 (Wideband Code Division Multiple Access/Time Division-Synchronous Code Division Multiple Access/Long Term Evolution, WCDMA/TD-SCDMA/LTE) 中基带芯片都用到的编码长度为 $m = 8$ 的CRC编码为例, 并行位宽 $w = 4$, CRC 编码生成多项式为 $G(x) = X^8 + X^7 + X^4 + X^3 + X + 1$, 信息序列 $M(x) = X^{13} + X^{12} + X^9 + X^8 + X^5 + X^4 + X^2 + X$, 对应序列为: $M(x) = (11001100110110)$, $G(x) = (110011011)$ 。本实例分零初态、非零初态两种情况。

1) 若零初态, $(X_m \cdots X_1) = (0 \cdots 0)$, 采用图1所示CRC编码方法计算后得 $R(x) = X^7 + X^4 + X^2 + X$, 对应 $R(x) = (10010110)$ 。

①采用并行CRC逆序校验方法解码:

步骤1 $(X_m \cdots X_1) = (0 \cdots 0)$; 信息序列 $M(x) = (11001100110110)$, 校验序列 $R(x) = (10010110)$, 无差错接收序列的逆序 $(a_1 \cdots a_l) = (0110100101101100110011)$; $w =$

4; $l = 22$; $m = 8$ 。

步骤2

$$P_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \Gamma = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, P_4 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

步骤3 调用 $R = \text{crc}^{-1}(m, w, P_w, a_1 \cdots a_l)$ 得 $R = (0 \cdots 0)$ 全零序列。

步骤4 $R = (X_1 \cdots X_m)$, CRC 校验正确。

正确解码。

②采用图2所示正序CRC校验方法解码: 无差错接收校验序列解码序列为 $M_R(x) = (b_0 \cdots b_{l-m-1} \cdots r_0)$, $M_R(x) = (1100110011011010010110)$, 计算得 $R = (00000000)$, 全零序列。

正确解码。

2) 若非零初态, 令 $(X_m \cdots X_1) = (00110110)$, 采用图1所示CRC编码方法计算后得 $R(x) = (01100011)$ 。

①采用并行CRC逆序校验方法解码:

步骤1中 $(a_1 \cdots a_l) = (1100011001101100110011)$; 步骤2中 P_1, Γ, P_4 与零初态中的1)例一致; 步骤3调用 $R = \text{crc}^{-1}(m, w, P_w, a_1 \cdots a_l)$ 计算得 $R = (01101100)$; 步骤4, $R = (X_1 \cdots X_m)$, CRC 校验正确。

正确解码。

②采用图2所示正序CRC校验方法解码: 无差错接收校验序列 $M_R(x) = (1100110011011001100011)$, 计算得 $R = (11110101)$, $R \neq (X_1 \cdots X_m)$ 。

错误解码。

因此, CRC 逆序校验方法对于零初态、非零初态CRC编码, 均可进行解码, 而CRC正序校验方法只能对零初态解码。

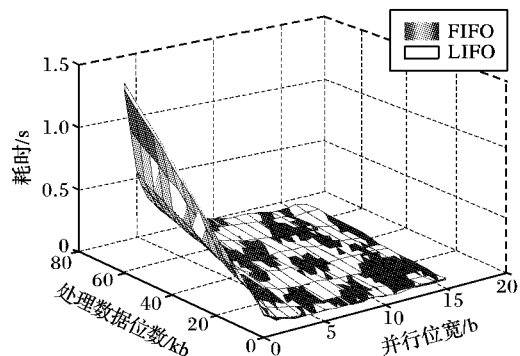


图6 不同数据长度、并行处理位宽下的CRC正、逆序校验耗时比较

为了能够更直观地观察快速CRC逆序校验算法在不同处理数据长度、不同并行位宽情况下的运行速度, 通过曲线拟合方法给出了零初态时并行CRC正序校验 (FIFO)^[7] 与快速CRC逆序校验 (LIFO) 耗时比较 (见图6), 图中处理数据轴表示输入处理的比特流长度 (5 kb, 10 kb, 20 kb, 30 kb, 40 kb, 50 kb, 60 kb, 65 kb)、并行位宽轴表示不同并行处理位数 (1, 2, 3, ..., 16 位, 为1位时, 即为文献[6]中描述的串行处理方法)、耗时轴表示计算所消耗的时间; 正序、逆序校验运算性能的两个曲面基本重合, 即耗时近似, 可得在相同处理数据长度、相同并行位宽时CRC正序、逆序运算具有类似的运算性能。

(下转第1865页)

身份标识的过滤技术的结合,在邮件分类中综合考虑邮件的内容特征与发件人身份标识特征;另一方面,借助用户反馈及时更新过滤方法的邮件分类知识,保证过滤方法对邮件特征变化的适应性。实验表明,该方法不仅能够有效地实现邮件的不同特征在邮件分类过程中的结合应用,提高邮件分类准确性,同时又能够降低邮件特征动态变化对邮件过滤性能的影响。

本文提出方法的下一步改进方向主要包括:利用网络安全相关技术完善用户反馈机制,进一步提升用户反馈机制的健壮性;完善用户信誉体系,以有效限制垃圾邮件制造者的身份标识更换行为。

参考文献:

- [1] 中国互联网协会反垃圾邮件工作委员会. 2010 年第四季度中国反垃圾邮件状况调查报告[EB/OL]. [2010-12-01]. <http://www.anti-spam.cn/>.
- [2] CARRERAS X, MRQUEZ L. Boosting trees for anti-spam email filtering [C]// Proceedings of the 4th International Conference on Recent Advances in Natural Language Processing. Washington, DC: IEEE Computer Society, 2001: 58-64.
- [3] GLYMIN M, ZIARKO W. Rough set approach to spam filter learning [C]// Proceedings of International Conference on Rough Sets and Intelligent Systems Paradigms. Washington, DC: IEEE Computer Society, 2007: 350-359.
- [4] THIAGO S, WALMIR M C. A review of machine learning approaches to spam filtering [J]. Expert Systems with Applications, 2009, 36(7): 10206-10222.
- [5] 惠享, 吴跃. 基于不完全朴素贝叶斯分类模型的垃圾邮件分类模型[J]. 计算机应用, 2009, 29(3): 902-904.
- [6] CHEN X L, LIU P Y, ZHU Z F. A method of spam filtering based

on weighted support vector machines [C]// Proceedings of the Second IEEE International Symposium on IT in Medicine and Education. Washington, DC: IEEE Computer Society, 2009: 947-950.

- [7] DONG D, ZHANG J. A spam filter system based on P2P architecture [C]// Proceedings of International Conference on Networking, Architecture and Storage. Washington, DC: IEEE Computer Society, 2008: 155-156.
- [8] 邓蔚, 秦志光, 刘峤, 等. 抗好词攻击的中文垃圾邮件过滤模型[J]. 电子测量与仪器学报, 2010, 24(12): 1146-1152.
- [9] LI Z, SHEN H. SOAP: a social network aided personalized and effective spam filter to clean your E-mail box [C]// Proceedings of the 32nd IEEE International Conference on Computer Communications. Washington, DC: IEEE Computer Society, 2011: 1835-1843.
- [10] KONG J, REZAEI B. Collaborative spam filtering using E-mail networks [J]. IEEE Computer, 2006, 12(1): 67-73.
- [11] SIRIVIANOS M, KIM K, YANG X. SocialFilter: introducing social trust to collaborative spam mitigation [C]// Proceedings of the 32nd IEEE International Conference on Computer Communications. Washington, DC: IEEE Computer Society, 2011: 2300-2308.
- [12] 唐晋韬, 王挺, 王戟. 适合复杂网络分析的最短路径近似算法[J]. 软件学报, 2011, 22(10): 2279-2290.
- [13] 中国教育和科研计算机网紧急响应组. 中文邮件样本集[EB/OL]. [2011-01-15]. <http://www.ccert.edu.cn/spam/sa/datasets.htm>.
- [14] 中文自然语言处理开放平台. 中文自然语言邮件集合[EB/OL]. [2011-01-15]. http://www.nlp.org.cn/docs/download.php?doc_id=1207.
- [15] 陶永才, 薛正元, 石磊. 基于 MapReduce 的贝叶斯垃圾邮件过滤机制[J]. 计算机应用, 2011, 31(9): 2412-2416.

(上接第 1835 页)

4 结语

本文提出了一种并行 CRC 逆序校验方法,采用 LIFO 的方式解码,即对接收序列进行逆序校验;对于零初态、非零初态 CRC 编码,均可进行校验,通过调整寄存器初态能够提高 CRC 编码信道传输的安全性,具有一定的防破解能力;可根据 w 大小任意拓展并行解码位数,无需预补零操作,简化了计算流程。综合以上特点,根据快速 CRC 逆序校验算法,通过硬件集成与实现^[13-15]鲁棒的、高速可变并行长度的 CRC 逆序解码器,提高解码的实时性需要进一步的探讨。

参考文献:

- [1] TANENBAUM A S. Computer networks [M]. 4th ed. New Jersey: Prentice Hall, 2003: 192-200.
- [2] STINSON D R. 密码学原理与实践[M]. 3 版. 冯登国, 译. 北京: 电子工业出版社, 2009.
- [3] PETERSON W W, BROWN D T. Cyclic codes for error detection [J]. Proceedings of the Institute of Radio Engineers, 1961, 49(1): 228-235.
- [4] GIUSEPPE C, GIUSEPPE, MARCO R. Parallel CRC realization [J]. IEEE Transactions on Computers, 2003, 52(10): 1312-1319.
- [5] CHENG C, PARHI K K. High-speed parallel CRC implementation based on unfolding, pipelining, and retiming [J]. IEEE Transac-

tions on Circuits and Systems, 2006, 53(10): 1017-1021.

- [6] STIGGE M, PLOTZ H, MULLER W, et al. Reversing CRC-theory and practice [EB/OL]. [2012-12-20]. <http://sar.informatik.hu-berlin.de/research/publications/>, 2006, 5.
- [7] 李双喜. 快速循环冗余校验编码方法及装置: 中国, 200910085524.4[P]. 2010-12-01.
- [8] GAJIC Z. 线性动态系统与信号[M]. 王立琦, 译. 西安: 西安交通大学出版社, 2004.
- [9] New Wave Instruments. Linear feedback shift registers [EB/OL]. [2012-12-20]. http://www.newwaveinstruments.com/resources/articles/m_sequence_linear_feedback_shift_register_lfsr.htm.
- [10] 臧玉亮, 韩文报. 线性反馈移位寄存器的差分能量攻击[J]. 电子与信息学报, 2009, 31(10): 2406-2410.
- [11] 白国强. 现代密码学 vs 集成电路技术[R]. 北京: 清华大学微电子学研究所, 2012.
- [12] 梁海华, 盘丽娜, 赵秀兰, 等. CRC 查询表及其并行矩阵生成方法[J]. 计算机科学, 2012, 39(S1): 154-158.
- [13] 王江, 张盛兵, 袁晓林. 面向 IP 复用的可配置并行 CRC 计算模块设计[J]. 计算机工程与科学, 2009, 31(1): 103-105.
- [14] 阳璞琼, 何怡刚, 谭阳红, 等. 超高频 RFID 系统 CRC 电路设计[J]. 电路与系统学报, 2009, 14(2): 18-21.
- [15] 袁海洋, 江先阳, 刘锋, 等. 应用于 ROHC 的 CRC 算法硬件实现[J]. 微电子学, 2011, 41(5): 736-740.