



中华人民共和国国家标准

GB/T 17710—2008/ISO/IEC 7064:2003
代替 GB/T 17710—1999

信息技术 安全技术 校验字符系统

Information technology—Security technique—
Check character systems

(ISO/IEC 7064:2003, IDT)

2008-07-16 发布

2008-12-01 实施

中华人民共和国国家质量监督检验检疫总局 发布
中国国家标准化管理委员会

目 次

| | |
|-------------------------------------|----|
| 前言 | I |
| 引言 | II |
| 1 范围 | 1 |
| 2 术语和定义 | 1 |
| 3 符号及其注释 | 2 |
| 4 系统类型 | 2 |
| 5 依从性及其冠名 | 3 |
| 6 纯系统的说明 | 4 |
| 7 带一位校验字符的纯系统的计算方法 | 5 |
| 8 带两位校验字符的纯系统的计算方法 | 7 |
| 9 混合系统说明 | 9 |
| 10 混合系数的计算方法 | 9 |
| 附录 A (资料性附录) 对各种应用选择校验字符系统的准则 | 11 |
| 附录 B (资料性附录) 非拉丁字母的校验字符系统 | 13 |
| 参考文献 | 14 |

前 言

本标准等同采用 ISO/IEC 7064:2003《信息技术 安全技术 校验字符系统》，仅有编辑性修改。本标准代替 GB/T 17710—1999。本标准与 GB/T 17710—1999 的区别如下：

- 标准的编排结构进行了调整；
- 对 2.1、2.2、2.3、2.6 的术语定义进行了修改。

本标准中的附录 A 和附录 B 是资料性附录。

本标准由中华人民共和国工业和信息化部提出。

本标准由全国信息技术标准化技术委员会归口。

本标准起草单位：中国电子技术标准化研究所、中国标准化研究院。

本标准主要起草人：陈星、杨建军、黄家英、史立武、张明天。

本标准所代替标准的历次版本发布情况为：

- GB/T 17710—1999。

引 言

校验字符系统标准化的需求出于如下考虑：

- a) 由于大量正在使用的系统中,许多系统具有相似的特征,而特征的许多的变化没有起到有效的作用;
- b) 现有的系统几乎没有经过严格的数学验证,有些还存在严重的缺陷;
- c) 系统的多样性削弱了校验字符系统的经济利益,而且经常妨碍对交换数据的校验。

因此,应选择一套小型兼容性系统,有效地满足各种应用的需要。该系统应经过验证,在各种应用的限制之内,高效地防止典型的复制和键入错误。

ISO 2180、ISO 2894(ISO 2894 已撤销)和 ISO 6166 也规定了校验字符系统,但它们只适用于特殊的领域,因此现有的系统无论如何不能获得本标准所规定的差错检测率。

附录 A 概述了为特定的应用而选用某一按本标准规定的校验字符系统时应考虑的准则。

附录 B 举例说明了在某些字母表数目超过 26 个字母的国家应用本标准的方法。

信息技术 安全技术

校验字符系统

1 范围

1.1 本标准规定了一组校验字符系统,它可以防止在复制或键入数据时产生的串的错误。串的长度可以是固定的或是可变的,包括以下字符集中的字符:

- a) 数字(10个数字:0~9);
- b) 字母(26个字母:A~Z);
- c) 字母数字(字母和数字)。

串中嵌入的空格和特殊字符忽略不计。

1.2 本标准为生成校验字符和校验串产品规约了一致性要求,这些产品采用了本标准所给出的系统。

1.3 这些校验字符系统能检查出下列错误:

- a) 所有的单一字符替换错误(即,单个字符被另一个字符所替换,如1234被错录为4234);
- b) 所有的或几乎所有的单一字符对换位置错误(即,相邻两个字符或隔一个字符的两个单一字符的位置互换,如12345被错录为12354或12543);
- c) 所有或几乎所有的循环移位错误(即,整个串被向左或向右循环移位);
- d) 大部分的双替换错误(即,在同一串中,分开的两处单一字符替换错误,如1234567被错录为7234587);
- e) 大部分的其他错误。

1.4 本标准不包括专门为下列目的而设计的系统:

- a) 既允许差错检测,又允许自动校正;
- b) 检测故意误用;
- c) 仅校验在机器之间交换的串。

1.5 本标准用于各组织之间的信息交换,极力推荐用于内部信息系统。

2 术语和定义

下列术语和定义适用于本标准。

2.1

校验字符 check character

可通过该串的数学关系来验证串的正确性所使用的附加字符。

2.2

校验字符系统 check character system

产生校验字符的和校验包含校验字符的串的一组规则。

2.3

补充校验字符 supplementary check character

不属于被保护串的字符集的校验字符。

2.4

模数 modulus

一个整数,它用作整除计算的除数以得到一个整数余数。