Algorithm

张昌硕 and 代金祥

2021 年 3 月 22 日

目录

1 数字签名

使用 SM3 国密摘要算法进行数字签名，如:

$$SM3(3312280576@qq.com) = eddcd1e894c7f181bec43b58dc1831fbeba5e23e8ad1778ee8faf2b0eb2209a3$$

2 预处理

2.1 签名预处理

将签名字符串转换为二维十进制 list(签名必须长度是 2 的倍数)，如将

$$eddcd1e894c7f181bec43b58dc1831fbeba5e23e8ad1778ee8faf2b0eb2209a3$$

转换为：

$$\begin{bmatrix} [14,13,13,12,13,1,14,8,9,4,12,7,15,1,8,1,11,14,12,4,3,11,5,8,13,12,1,8,3,1,15,11] \\ [14,11,10,5,14,2,3,14,8,10,13,1,7,7,8,14,14,8,15,10,15,2,11,0,14,11,2,2,0,9,10,3] \end{bmatrix} \tag{1}$$

2.2 编码分区

将字符 ch 分区到 $i = unicode(ch)\%n$，其中 n 为 list 的列数。

3 字形添加信息

SV G 是一种基于 XML 语法的图像格式，记录内容为对图像的形状描述。Fontforge.export() 导出的 svg 图片的字形信息均在 xml 的基本形状的 < path > 元素中，其中 d 属性只包括 M, h, v, l, q, t, z 命令。具体请看此链接：svg 图片 Path 标签用法

3.1 q 命令添加信息

q 命令为绘制二阶贝塞尔曲线，由于终点位置不能改变我们将信息加入到控制点的信息中，并考虑到改动幅度应与曲线长度基本成正比，具体变化为：

$$\begin{cases} ctrl_x += list[0][i] * (dx//\alpha)//2 + 1 \\ ctrl_y += list[1][i] * (dy//\alpha)//2 + 1 \end{cases} \tag{2}$$

其中 α 为自定义参数（可改变以得到想要的字体），dx，dy 为 q 命令的第三、四个参数，i 为待变化字所属的编码分区。

3.2 h 命令添加信息

考虑将 h 命令直线转换为三阶贝塞尔曲线，$(h\ dx)$ 转换为：(c $ctrl_x^1$ $ctrl_y^1$ $ctrl_x^2$ $ctrl_y^2$ dx 0)，具体变化为：

$$\begin{cases} ctrl_x^1 = dx//(2 + list[(i+1)\%20][1]) \\ ctrl_x^2 = dx - ctrl_x^1 \\ ctrl_y^1 = (dx//\beta) * (list[i][1] - 8) \\ ctrl_y^2 = -ctrl_y^1 \end{cases} \tag{3}$$

其中 β 为自定义参数（可改变以得到想要的字体）

3.3 v 命令添加信息

考虑将 v 命令直线转换为三阶贝塞尔曲线，$(h\ dx)$ 转换为：$(c\ ctrl_x^1\ ctrl_y^1\ ctrl_x^2\ ctrl_y^2\ 0\ dy)$，具体变化为：

$$\begin{cases} ctrl_x^1 = (dy//\beta) * (list[i][0] - 8) \\ ctrl_x^2 = -ctrl_x^1 \\ ctrl_y^1 = dy//(2 + list[(i+1)\%20][0]) \\ ctrl_y^2 = dy - ctrl_y^1 \end{cases} \tag{4}$$

3.4 l 命令添加信息

考虑将 l 命令直线转换为二阶贝塞尔曲线，即 $(l\ dx\ dy)$ 变化为 q 命令 $(q\ ctrl_x\ ctrl_y\ dx\ dy)$，具体变化为：

$$\begin{cases} ctrl_x = dx//2 + list[0][i] * (dx//\beta)//2 \\ ctrl_y = dy//2 + list[1][i] * (dy//\beta)//2 \end{cases} \tag{5}$$