基于现场可编程门阵列的手机短信息混沌加密系统设计方案及硬件实现*

潘晶 齐娜 薛兵兵 丁群†

(黑龙江大学电子工程学院, 校信号与信息处理重点实验室, 哈尔滨 150080)

(2011 年 12 月 8 日收到; 2012 年 2 月 28 日收到修改稿)

手机的普及使得个人信息安全问题受到广泛关注, 其中手机短信息的安全性尤为重要. 本文致力于设计实现手机短信息加密与安全传输的硬件系统, 采用混沌 A5/1 混合算法, 提出一种基于现场可编程门阵列 (FPGA) 的手机短信息加密系统设计方案. 使用由 Logistic 混沌序列做初始密钥而改进的 A5/1 混合算法作为加密算法, 分析其伪随机性并证明圆周相关与线性相关的关系; 采用 SIM300 模块设计实现手机功能, 仿真普通手机短信息和加密短信息的传输; 开发一套软件测试平台, 可以在计算机上呈现硬件系统的测试结果. 经测试表明, 本文提出并实现的硬件系统可以加密手机短信息并保证其正常传输, 从而提高了手机短信息的安全性.

关键词: 混沌 A5/1 混合算法, 圆周相关, 手机短信息硬件加密, 软件测试平台

PACS: 05.45.Vx, 84.40.Ua, 43.38.Si

1 引 言

随着通信技术的进步, 移动设备手机的普及, 信息在传输过程中的安全问题越来越受到广泛的关注, 其中与人们密切相关的隐私问题就是短信息的安全性. 由于短信息在传送过程中需要经过基站, 而基站一旦被攻破, 个人的短信息对于攻击者而言就是透明的, 不具有安全性, 所以这种缺陷将会成为威胁人们隐私安全的首要问题. 关于信息安全问题, 现如今已经有许多的经典密码学算法应用在日常生活中. 从 20 世纪 90 年代, 混沌作为一门新兴学科, 由于其内在随机性, 对初始条件敏感性等一系列类似密码学的特征, 使其成为信息安全和保密通信研究者们的一大研究热点. 尤其是在 1989 年, Pecora 和 Carroll 发现并提出了基于混沌同步的保密通信方案后, 混沌保密通信的研究俨然已经成为国际电子通信领域的一个热门课题 [1]. 近年来, 许多学者致力于研究混沌加密算法 [2−5], 还有一些学者将混沌加密算法应用到了不同的领域中 [6], 比如 2002 年 Tang 等提出了在混沌光通信中的基于混沌调制的信息加解密, 文中描述的是针对光通信中采用混沌调制从而实现信息的加解密过程 [7], 2009 年周武杰等设计实现了混沌数字通信系统 [8], 2010 年张朝霞等用硬件实现了语音无线混沌通信 [9], 同年, 晋建秀和丘水生等研究了物理混沌混合图像加密系统 [10], 对于手机短信的研究, 有吴日华等研究过手机短信网络生长的过程 [11]. 而对于基于混沌的加密算法在手机短信中的研究, 即手机短信息加解密方面却鲜有研究, 更确切地说, 有一些理论方面的研究主要是针对算法而不是系统设计与硬件实现. 比如 2007 年胡国香提出了基于椭圆曲线公钥密码体制的手机短信加密方案, 该方案只是从理论上进行了推导和软件仿真, 并未给出具体的硬件实现 [12]; 当然, 近年来也有人尝试在硬件实现方面仿真手机系统, 比如 2008 年陈滟涛等提出了基于 SIM300 的短信传输系统的设计与实现, 但是该方案只是采用硬件实现了短信传输系统

* 国家自然科学基金 (批准号: 61072072) 和黑龙江大学学生创新实验室项目 (批准号: CX11175) 资助的课题.

† E-mail: qunding@yahoo.cn

© 2012 中国物理学会 Chinese Physical Society

并未对短信息进行加密, 从而不能保证信息的安全传输 [13]. 通过对国内外许多学者在信息加解密研究的理论与仿真的了解, 以及对手机短信息通信系统的研究, 我们致力于弥补两者没有有机的结合成为统一的硬件系统的空缺, 将基于混沌的加密算法引入对短信息的加密方案中. 我们采用现场可编程门阵列 (FPGA) 芯片设计了混沌 A5/1 混合算法作为加密核, 是手机短信息加密的研究基础, 硬件实现中采用 SIM300 模块仿真普通手机短信息收发功能, 从而确保本文提出的硬件系统实现对手机短信息的加解密和正常传输.

2 基于混沌 A5/1 混合加密的算法设计

2.1 Logistic 映射及数字化 Logistic 序列

基于混沌 A5/1 混合加密算法的设计, 采用混沌序列作为初始密钥, 选择采用 Logistic 映射, 其表达式如下 [14]:

$$x_{n+1} = \mu x_n(1-x_n), \quad \mu \in (0,4), \quad x_n \in (0,1), \tag{1}$$

其中 x_n 为 Logistic 映射的状态值, 当 Logistic 映射参数 $\mu \in (3.57, 4)$, 进入混沌状态. 我们可以选择参数 μ 和 Logistic 映射迭代初始值作为混沌加密算法的密钥, 在本系统中采用用户动态自定义密码的方法来设置混沌加密算法的密钥, 通过用户每次动态输入的密钥, 加上混沌映射对初值敏感性的特性, 从而达到 "一次一密" 效果 [15].

我们知道, 以上介绍的是混沌系统中常用的一维离散混沌模型, 但是此系统产生的仍然是实值的序列, 在将其应用到实际系统中时, 我们使用的 Logistic 混沌序列必须根据需要进行二值化处理. 关于混沌序列的二值化处理, 许多文献都给出了不同的方法 [16−18], 均可以将混沌信号 $x(n)$ 转换成二值序列流 $s(n)$, 此处我们使用的是引入量化函数 $T[x(n)]$[19,20]. 量化函数 $T[x(n)]$ 定义如下:

$$T[x(n)] = \begin{cases} 0, & x(n) \in \bigcup_{k=0}^{2^m-1} I_{2k}^m, \\ 1, & x(n) \in \bigcup_{k=0}^{2^m-1} I_{2k+1}^m, \end{cases} \tag{2}$$

其中 $m > 0$ 并为任意整数, $I_0^m, I_1^m, I_2^m, \cdots$ 是 [0, 1] 区间的 2^m 个连续的等分区间. 如果转换值落在量化函数以奇数为初始位的区间, 则量化后值为 1; 若落在以偶数为初始位区间则量化后值为 0. 由于混沌信号 $\{x(n)\}$ 具有良好的随机统计特性, 这样所转换后的 $\{s(n)\}$ 在理论上具有均衡的 0—1 比和自相关等优良的统计特性, 这也将从实验进一步得到验证.

本文采用先前工作中用到的设计 [21], 用 (2) 式作为系统实现式进行转换并得出具体的序列输出, 具体设计如下.

当取值 $X = \{x(n)|n = 0,1,2,\cdots, x(n) \in [0,1]\}$, 转化后二值序列为: $S = \{s(n)|n = 0,1,2,\cdots, s(n) \in \{0,1\}\}$, 区间单位间隔 $\Delta = 1/2^m$, 其中 m 为任意正整数, 整个区间为 $[0\Delta 1\Delta) \cup [1\Delta 2\Delta) \cup [2\Delta 3\Delta) \cup \cdots \cup [(2^m-1)\Delta 2^m\Delta]$, 这里取 $k = 0,1,2,\cdots 2^m - 1$, 则转换函数 (2) 式可以由以下 (3) 式描述:

$$T[x(n)] = \begin{cases} 0, x(n) \in [2k\Delta(2k+1)\Delta), \\ 1, x(n) \in [(2k+1)\Delta(2k+2)\Delta]. \end{cases} \tag{3}$$

为了简化设计和易于电路实现, 将 (3) 式中的 Δ 线性转成 (4) 式所示:

$$T[x(n)] = \begin{cases} 0, 2^m x(n) \in [2k(2k+1)), \\ 1, 2^m x(n) \in [(2k+1)(2k+2)]. \end{cases} \tag{4}$$

这样处理后, 即新的量化单位 $\Delta = 1$, 整个转换区间为 $[0\,1) \cup [12) \cup [23) \cup \cdots \cup [(2^m-1)2^m]$, 这样可以利用 $2^m x(n)$ 乘积整数位来确定转换区间, 根据其乘积整数位个位的奇偶性来确定序列输出为 0 或者 1, 这种处理使得硬件上只需要移位寄存器完成 $2^m x(n)$ 功能, 位抽取器完成个位奇偶判断功能, 即由筒形移位寄存器和位抽取器两个器件就可以完成 (2) 式中转换函数功能, 完成混沌序列的二值化处理. 避免复杂运算, 使电路简化. 图 1,2 分别给出了 Logistic 混沌序列量化前和量化后的输出波形 [14].

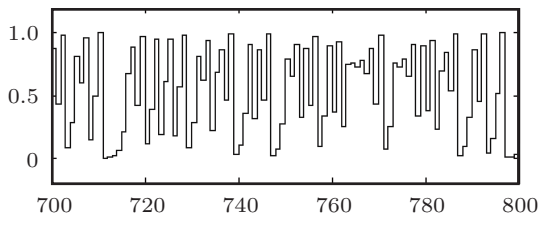

图 1 Logistic 混沌序列量化前波形

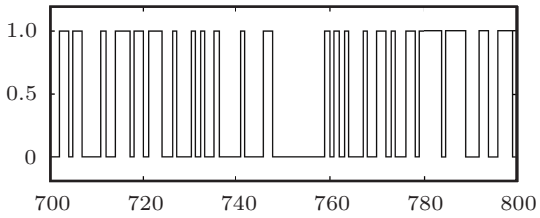

图 2 Logistic 混沌序列量化后波形

2.2 基于混沌 A5/1 混合加密的算法设计

加密算法依赖于密码学核心理论、安全体系结构、网络安全通信协议等, 其中密码的选取与设计是关键. 在标准的流密码中有 A5 系列, E0 码、RC4, Helix, SEA 码, WAKE 码等 [22]. 这些密码中, A5/1 常用于 GSM, E0 用于蓝牙, RC4 用于 IEEE 802.11 b 和其他标准中, Helix 是一种面向字的流码, 它可以提供消息鉴别码 MAC 功能. 由于本系统是采用 GSM/GPRS 的无线传输模块 SIM300 模块设计实现的, 所以在该加密核中应选用 A5 系列, 本设计选择 A5/1 加密算法, 不仅因为它的硬件设计简单, 技术比较成熟和通过所有统计测试, 更重要的是用 FPGA 实现此方案, 具有速度快, 配置灵活, 易于修改和软件化的优点. 采用 A5/1 做算法的基本框架, 其算法框图如图 3 所示 [23,24], 用前文介绍的混沌序列输出初始密钥, 改进 A5/1 系列流密码进行加密. 这种算法设计是考虑到由于量化等原因混沌序列应用到数字通信系统中会丢失本身的一些混沌特性导致安全性降低 [25], 所以将其结合传统的 A5/1 密码算法进行改进, 而 A5/1 算法是欧洲数字蜂窝移动电话系统 GSM 中采用的流密码加密算法, 具有广泛的应用, 但是它在初始化过程中存在缺陷, 即密钥比特和帧比特都是线性填充, 容易被相关攻击 [26], 此处将其与非线性动力系统即混沌系统产生的混沌流密码结合, 用混沌密码进行初始化, 可以确保安全稳定, 这样两者可以相互补充改进, 效果更好.

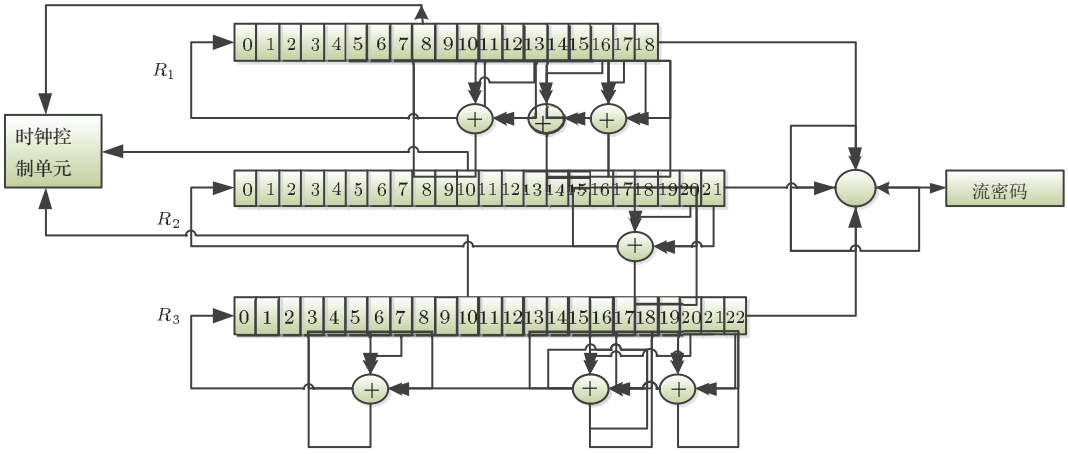

图 3 A5/1 算法框图

本设计方案中加/解密算法模块是以混沌算法、数字电路理论、复杂度为基本思想设计的. 图 4 所示为加密算法设计方案原理图, 加密核部分内嵌的就是实现对手机短信进行加密、解密处理的模块, 其内部为混沌 A5/1 混合算法, 由于 Logistic 混沌序列为 A5/1 序列密码提供良好的初始密钥, 这样改进的 A5/1 序列密码有着高保密强度、高复杂度和对初始数据极其敏感的特点, 混沌 A5/1 混合加密原理如图 5 所示. 将明文序列 $m = \{m_i\}$ 用密钥序列 $z = \{z_i\}$ 逐位加密, 得到密文序列 $c = \{c_i\}$ 的密码, 在实用的序列密码中, 加密变换为 $c_i = m_i \oplus z_i$, 解密变换为 $m_i = c_i \oplus z_i$. 作为序列密码模型, 对于每一个由混沌系统产生的初始密钥 k, 可通过算法确定一个密钥序列 $z = \{z_i\}$. 序列密码的安全性主要取决于密钥序列的安全性. 当 $z = \{z_i\}$ 为均匀分布的二进制随机序列时, 则密码系统为一次一密系统, 因此是很难被攻破的. 而且采用高性能的 FPGA 技术, 为后续系统升级提供在不改变电路的情况下对加密核的替换.

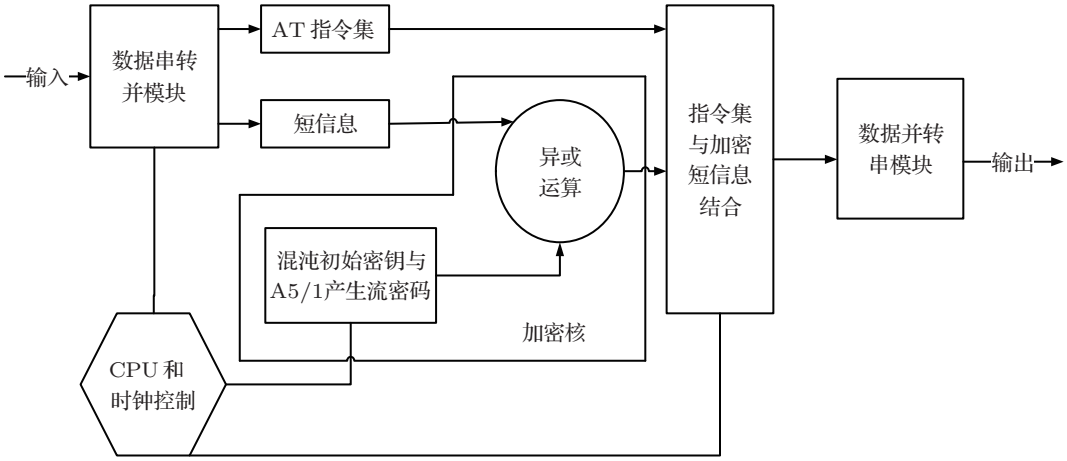

图 4 加密算法设计原理图

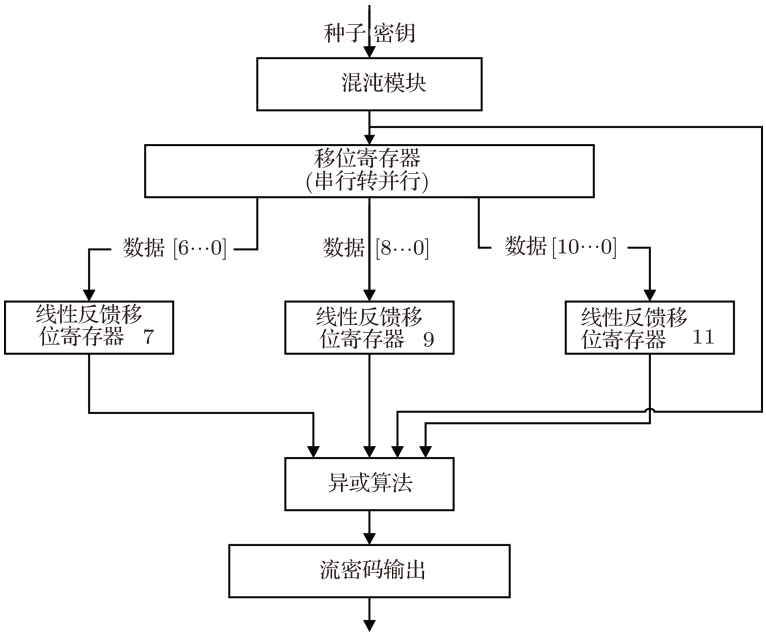

图 5 混沌 +A5/1 加密原理图

序列密码既流密码, 本系统运用了三个线性反馈移位寄存器, 分别为 7 级、9 级和 11 级. 线性反馈移位寄存器更适合硬件的实现, 能产生大周期的具有很好的统计特性和伪随机性序列. 经过三种线性反馈移位寄存器得出的输出序列仿真图, 如图 6 所示.

本文设计的系统采用基于混沌 A5/1 算法, 由我们之前研究搭建的一维 Logistic 混沌系统产生数字化混沌序列模块, 产生初始密钥 [27], 将这个初始密钥作为加/解密密钥, 具有密钥空间大, 并且伪随机性好的优势, 具体分析包括平衡性检验、游程分析和相关性分析.

平衡性检验是检验是否类似于随机系统, 在整个状态空间服从均匀分布的特点, 通过取不同长度、不同初值的序列, 经过实验结果表明序列的 0 与 1 数目几乎趋于平衡.

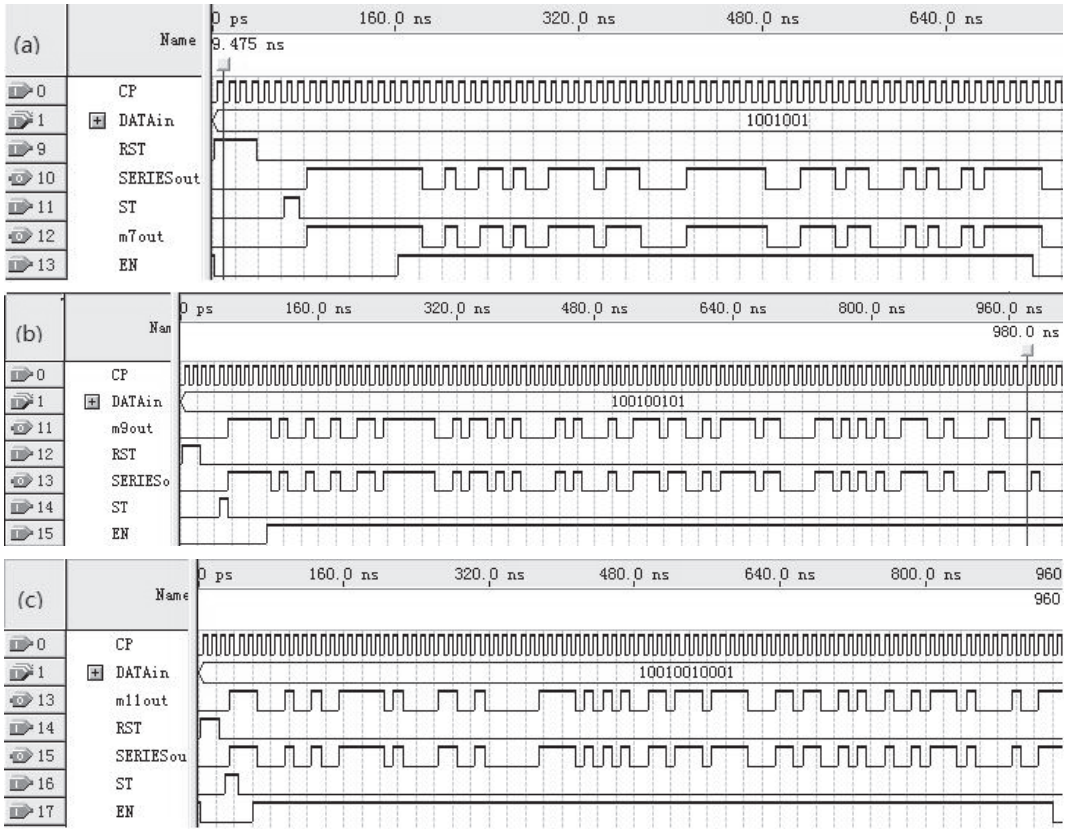

图 6 线性反馈移位寄存器模块时序仿真图 (a) 7 级; (b) 9 级; (c) 11 级

不平衡度的计算公式为

$$\frac{(Q_1 - Q_0)}{N}\%, \tag{5}$$

其中 Q_1 为实际观测序列为 1 的个数, Q_0 为实际观测序列为 0 的个数, N 为实际观测序列总个数. 根据样本实际观察次数与按理论模型求得次数之间相符程度来检验该模型是否成立. 本次实验是以统计量 χ^2 分布作为检验的依据, 构造 χ^2 统计量公式为

$$\chi^2 = \sum_{i=1}^{k} \frac{|Q_i - E_i|^2}{E_i}, \tag{6}$$

此式服从自由度为 $k-m$ 的 χ^2 分布. 其中 k 是观测项目, m 为理论模型的变量数目. 在 0 与 1 序列中 $k=2$, $m=1$, 它服从自由度为 1 的 χ^2 分布. 各项目的实际观测次数为 $Q_1, Q_2, \cdots, Q_K$, 各项目的理论次数为 $E_1, E_2, \cdots, E_K$, 如果该统计量的 χ^2 值小于 3.8415 就表明通过检验了, 因为对实验数据进行自由度为 1 的 χ^2 检验, 当显著性水平 5%, 对应的 χ^2 值为 3.8415, 结果表明通过率为 99%[27] .

游程特性的分析是对序列游程特性分析, 结果表明实际游程特性与理论游程特性接近, 即序列中长度为 1 的游程约占游程总数的 1/2, 长度为 2 的游程约占游程总数的 $1/2^2$, 长度为 3 的游程约占游程总数的 $1/2^3 \cdots$, 长度为 k 的游程约占游程总数的 $1/2^k$, 如此递减. 对于任意长度 0 的游程个数和 1 的游程个数近似相等 [27].

相关性分析这里引入的是圆周相关, 由于实际应用中序列不可能无限长, 序列的好坏也取决于计算上的不可预测. 通常的做法是取一个有限的计算系统能够承受的相关序列, 因此在满足一定条件下, 圆周相关可以取代线性相关更具有普遍性. 对此, 本文给出了证明.

结论 已知两个实序列 $X = \{x_1, x_2, \cdots, x_{N_1}\}$, $Y = \{y_1, y_2, \cdots, y_{N_2}\}$, 它们的点数分别为 N_1, N_2, 当两序列补零到序列点数大于或等于 (N_1+N_2-1) 点时, 可以用两序列的圆周相关来代替线性相关.

证明 1) 首先给出线性相关公式, 对于两个实序列 X 和 Y 做两序列相关, 以哪个序列作为基准

序列, 则线性相关后的非零点个数与其点数相同, 根据线性相关公式可知:

$$r_l(m) = \sum_{n=-\infty}^{n=+\infty} x(n)y(n-m) = \sum_{n=0}^{N_1-1} x(n)y(n-m), \tag{7}$$

X 的非零区间为 $0 \leqslant n \leqslant N_1-1$, Y 的非零区间 $0 \leqslant n-m \leqslant N_2-1$, $r_l(m)$ 可以是 N_1 或 N_2 点, 是一个有用非零点的个数不超过 (N_1+N_2-1) 点的有限长序列.

2) 再给出圆周相关, 设点数为 L 点的圆周相关, 再讨论 L 取何值时圆周相关才能表示线性相关. 定义符号 ϑ 表示圆周相关. $r(m) = x(n)\vartheta y(n)$ 表示 X 和 Y 的圆周相关, 先将两者均看成 L 点的序列, 令

$$\begin{cases} x(n) = \begin{cases} x(n), & 0 \leqslant n \leqslant N_1-1, \\ 0, & N_1 \leqslant n \leqslant L-1, \end{cases} \\ y(n) = \begin{cases} y(n), & 0 \leqslant n \leqslant N_2-1, \\ 0, & N_2 \leqslant n \leqslant L-1, \end{cases} \end{cases} \tag{8}$$

在 X 中补 $(L-N_1)$ 个零点, 在 Y 中补 $(L-N_2)$ 个零点.

$$r(m) = \left[\sum_{n=0}^{L-1} x(n)y((n-m))_L\right] R_L(m), \tag{9}$$

将 Y 变成 L 点周期延拓序列, 即 $\tilde{y}(n) = y((n))_L = \sum_{P=-\infty}^{+\infty} y(n+pL)$. 代入上式得:

$$\begin{aligned} r(m) &= \left[\sum_{n=0}^{L-1} x(n)y((n-m))_L\right] R_L(m) \\ &= \left[\sum_{n=0}^{L-1} x(n) \sum_{p=-\infty}^{+\infty} y(n+pL-m)\right] \\ &\quad \times R_L(m) \\ &= \left[\sum_{p=-\infty}^{+\infty} \sum_{n=0}^{L-1} x(n)y(n+pL-m)\right] \\ &\quad \times R_L(m) \\ &= \left[\sum_{p=-\infty}^{+\infty} r_l(m-pL)\right] R_L(m), \end{aligned} \tag{10}$$

L 点圆周相关 $r(m)$ 是线性相关 $r_L(m)$ 以 L 为周期进行延拓的序列的主值序列, $r_L(m)$ 最多有 (N_1+N_2-1) 个有用非零值, 所以 $L \geqslant N_1+N_2-1$, 这时各延拓周期才不会交叠, $r(m)$ 的前 (N_1+N_2-1) 个值正好是 $r(m)$ 的全部非零值, 也是 $r_L(m)$, 证毕.

因此测试相关性所需的自相关和互相关的估值公式如下:

自相关函数的估值公式

$$R_{XX}(m) = \frac{1}{N} \sum_{n=0}^{N-1} x(n)x((n+m))_N R_N(m), \tag{11}$$

互相关函数的估值公式

$$R_{XY}(m) = \frac{1}{N} \sum_{n=0}^{N-1} y(n)x((n+m))_N R_N(m). \tag{12}$$

因为不同的初值产生不同的混沌序列, 当设定两个初始值后, 可观测两个序列的互相关特性, 并利用自相关公式与互相关公式进行仿真, 得到本文所用的混沌序列自相关特性与互相关特性 [14,27]. 性质较好, 自相关特性在 0 值处峰值尖锐, 其他值近似为 0, 类似于 δ 函数; 互相关特性类似于均值为 0 的白噪声, 具有较好的互相关特性. 还有序列的周期性, 我们希望用来加密的序列尽量没周期, 关于这方面的讨论, 我们也有专门的研究小组进行研究 [21,28].

3 基于 FPGA 的手机短信息混沌加密硬件系统的建立

3.1 硬件系统的总体设计方案

基于我们对手机短信息加密传输系统的设计, FPGA 模块中主要包括串口、控制模块、短信息处理模块和数据加/解密核. 控制模块对加密级别、协议、以及整个运行时序进行控制. FPGA 模块中的加密模块对短信息数据进行流加密, 保证了无线传输的识别. 采用的是混沌与 A5/1 算法混合算法, 在第二章中有所介绍. 基于 FPGA 和混沌加密算法的手机短信加密系统开发板的原理框图如图 7 所示. 该总体设计方案, 可以在实验调试中完成短信息的读写、信息控制及处理、加密与非加密控制、加/解密传输收发等多种功能, 实现了系统的设计目的.

3.2 手机短信息收发格式处理

手机发送短消息通常有两种模式, TEXT 模式和 PDU 模式. 使用 Text 模式收发短信代码简单, 实现起来十分容易, 但最大的缺点是不能收发中文短信; 而 PDU 模式支持中文短信. PDU 模式收发短信可以使用 3 种编码: 7-bit, 8-bit 和 UCS2 编码. 7-bit 编码用于发送普通的 ASCII 字符, 8-bit 编码通常用于发送数据消息, UCS2 编码用于发送 Unicode字符 [29].

(1) TEXT 模式发送/接收信息模式, 我们总结归纳为图 8 所示.

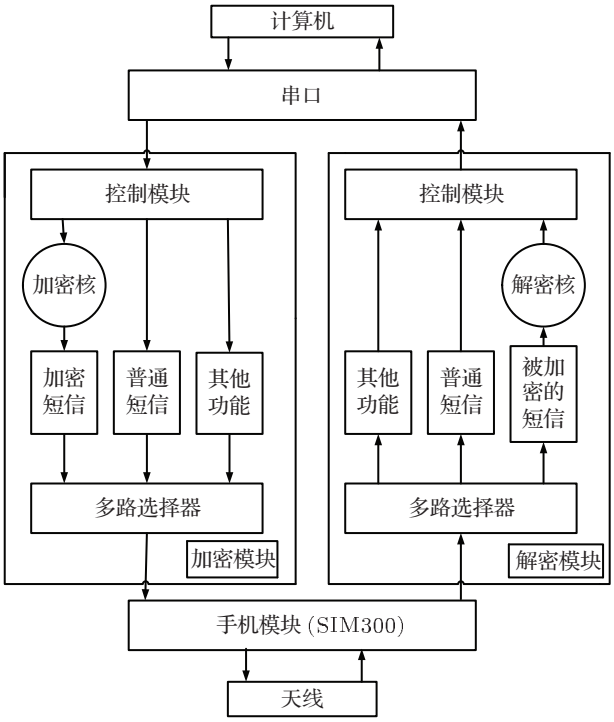

图 7 系统开发板的总体设计原理图

2) 本系统用到 PDU 模式, 详细介绍一下 PDU 模式发送短信:

第一步: at + cmgf = 0, 如果返回 ok 则继续

第二步: 手机号码处理: 用字符串 phone

a) 将手机号码去掉 + 号, 看看长度是否为偶数, 如果不是, 最后添加 F, 即 phone = "8613602433649" ⇒ phone = "8613602433649F"; b) 将手机号码奇数位和偶数位交换, ⇒ phone = "683106423346F9";

第三步: 短信息部分处理: 用字符串 msg 表示

a) 转字符串转换为 Unicode 代码, 例如 "工作愉快!" 的 unicode 代码为 5DE54F5C61095FEBFF01;

b) 将 msg 长度除 2, 保留两位 16 进制数, 即 5DE54F5C61095FEBFF01 = 20/2 => "0A", 再加上 msg, ⇒ msg = "0A5DE54F5C61095FEBFF01";

第四步: 组合

a) 手机号码前加上字符串 11000D91(1100: 固定, 0D: 手机号码的长度, 不算 + 号, 十六进制表示, 91: 发送到手机为 91, 发送到小灵通为 81), 即 phone = "11000D91" + phone ⇒ 11000D91683106423346F9;

b) 手机号码后加上 000800 和刚才的短信息内容, 000800 也写入就可以了, 即 phone = phone + "000800" + msg, 即 11000D91683106423346F9 + 000800 + 0A5DE54F5C61095FEBFF01 ⇒ phone = 11000D91683106423346F90008000A5DE54F5C61095FEBFF01;

c) phone 长度除以 2, 格式化成 2 位的十进制数, 即 11000D91683106423346F90008000A5DE54F5C61095FEBFF01⇒50 位/2⇒25.

第五步: AT+CMGS=k⟨ 回车 ⟩; > addr + phone⟨Ctrl +Z 发送 ⟩.

同理, 反过程为 PDU 格式接收短信处理方式, 本设计采用 PDU 格式收发短信, 这样手机在能够显示数字和字母的情况下还能编辑汉字.

3.3 软件测试平台与系统硬件实现

为了便于系统开发测试, 我们在电脑上设计了系统的软件测试平台界面如图 9 所示. 本文硬件实现的系统实物图如图 10 所示. 采用以上介绍的设计方案完成的系统使用高性能的 FPGA 芯片, 加/解密算法均采用 IP 核下载到 FPGA 中, 以后进行系统加密算法更新的时候不用更改任何电路, 只需要把测试好的 IP 核下载到 FPGA 芯片中即可完成, 这既为用户节省成本也可以实现不同的算法下载, 且所采用的技术均经过测试, 可以实现实时加密, 解密和安全认证等功能.

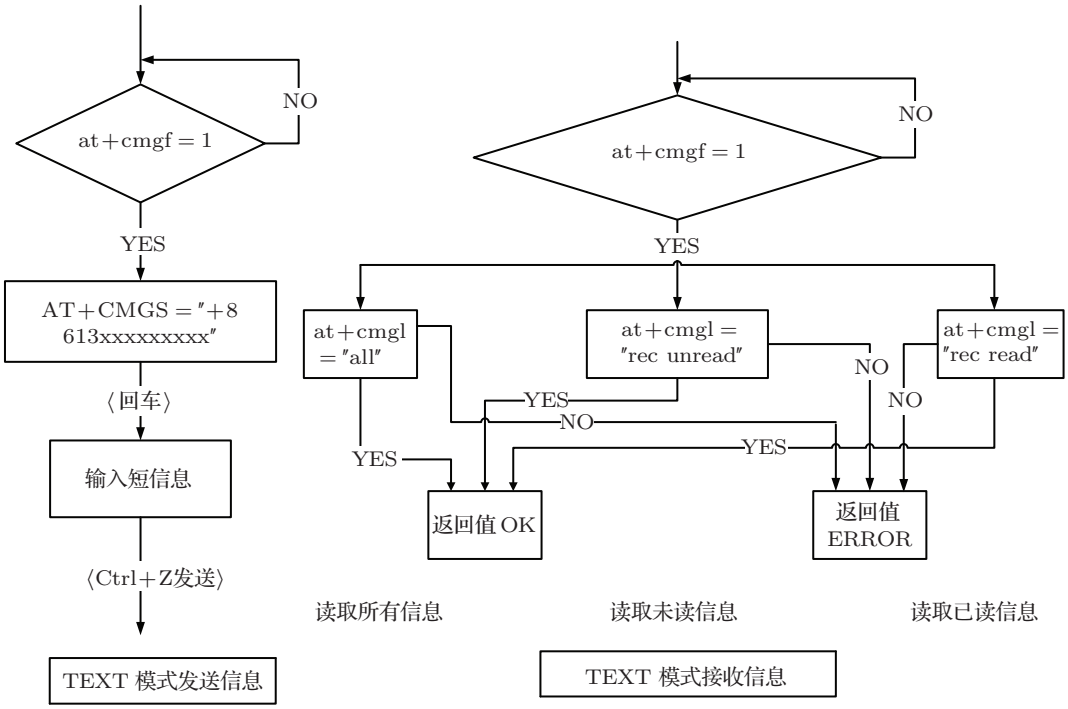

图 8 TEXT 模式发送接收信息图示

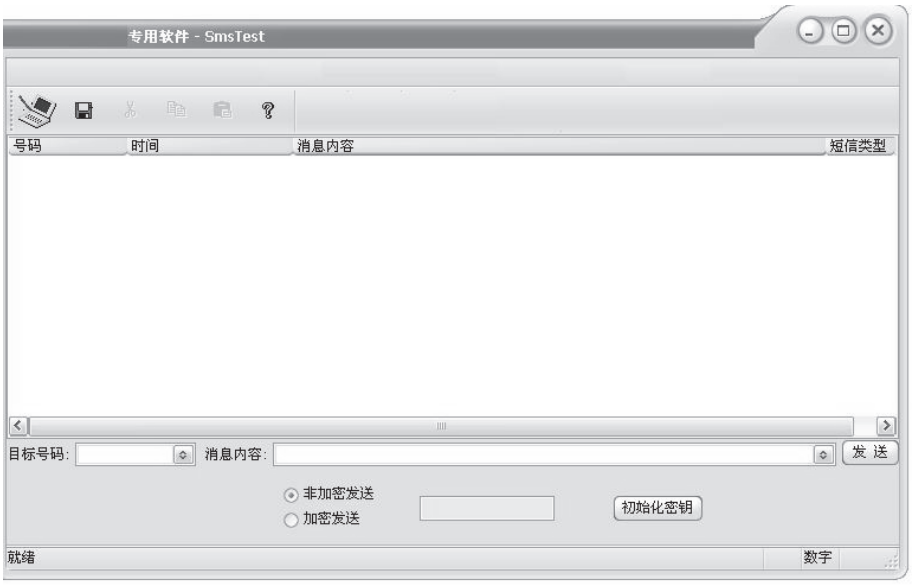

图 9 本系统开发的软件测试界面

4 系统测试分析与讨论

根据系统的硬件实现, 测试分析与讨论系统性能, 验证此手机短信息加密传输系统的开发板可以实现对短信息的加密和解密传输, 并且通过测试调试, 可以与普通手机用户实现通信, 从而保证短信的安全性、可靠性.

测试过程:

将硬件系统连接计算机, 采用软件平台来测试模仿手机短信息的收发, 并用普通手机作为第三方来验证短信息的保密性.

用户 1 和用户 2 是使用本加密短信息传输系

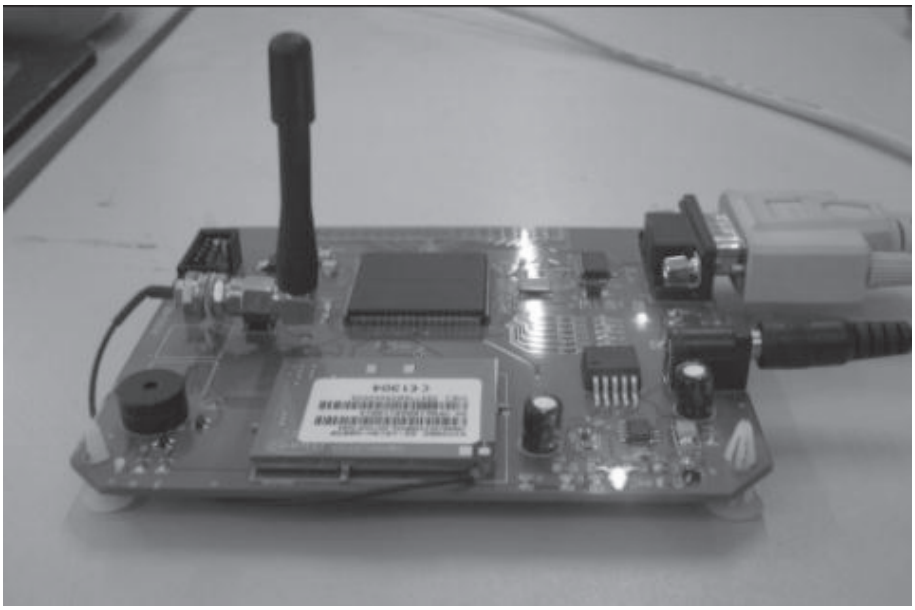

图 10 系统硬件实现实物图

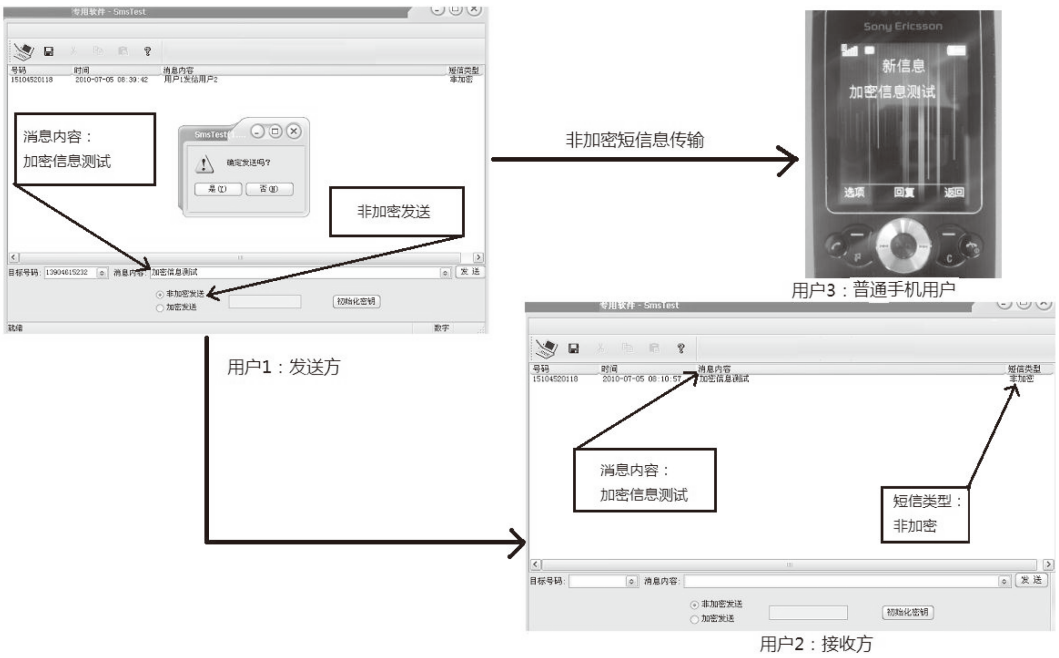

图 11 系统测试一: 非加密手机短信息测试图

图 12 系统测试二: 向普通手机发送加密短信息测试图

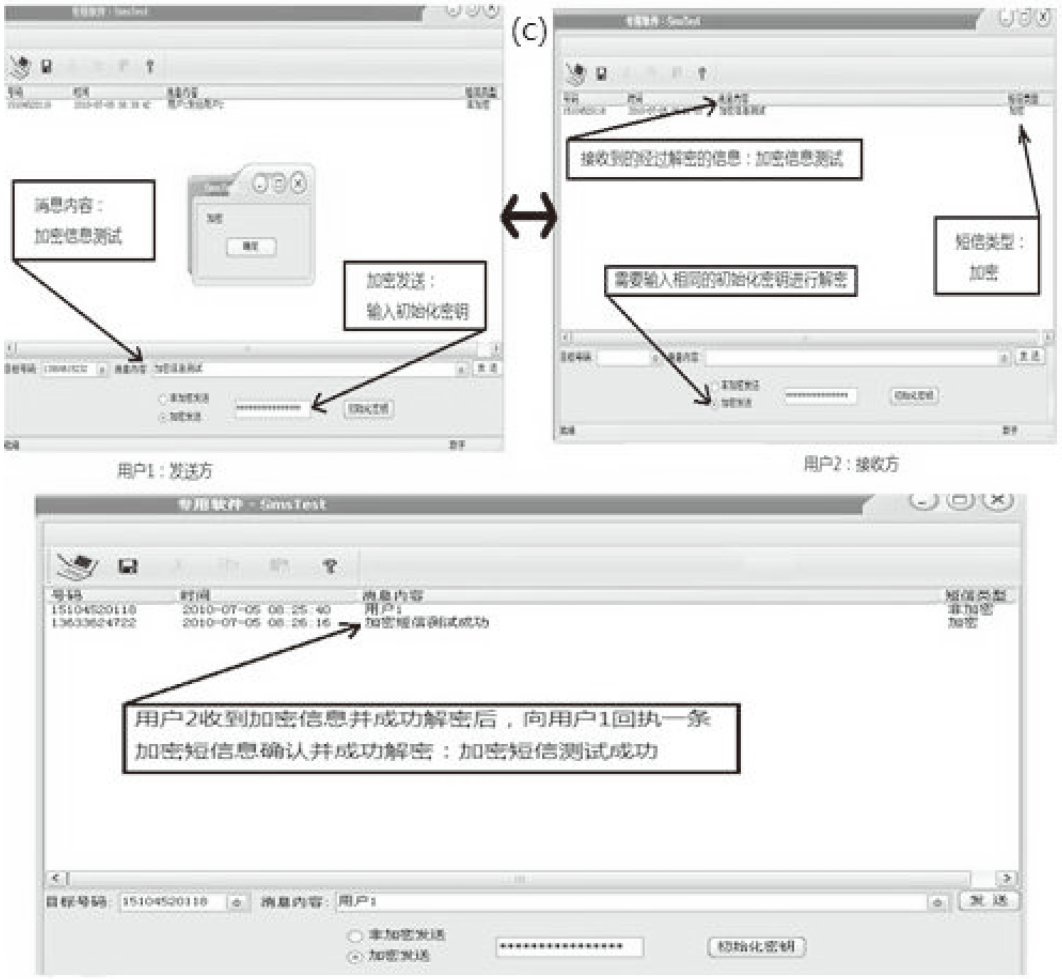

图 13 系统测试三: 加密短信息收发测试图

统的显示界面, 普通手机用户作为用户端 3, 我们使用的用户 1、用户 2 和手机用户 3 三者之间均能进行普通非加密短信息的收发, 如图 11 所示. 用户 1 将加密短信发给手机用户 3, 显示收到的短信息是乱码信息, 如图 12 所示. 用户 1 发送加密信息, 只有在用户 2 输入一致的初始化密钥后, 才会正确的解出完整的信息, 此时用户 2 再给用户 1 发送回执信息, 实现手机短信息的加密传输与解密接收功能, 如图 13 所示.

经过测试表明, 本文提出并实现的手机短信息加密系统可以模拟普通手机短信息收发功能, 能够与普通手机进行非加密短信息和加密短信息的正常通信. 收发双方需要用相同的密码进行初始化, 才能正确解密出短信息, 从而保证了手机短信息的安全性. 通过实验, 证明了本文所提出的系统能够填补将手机短信息加密与硬件实现两者有机的结合成为统一的硬件系统的空缺, 实现了本文的研究目标, 本研究为将来手机短信息加密系统的广泛应用提供一定的理论与实践相结合的研究基础.

5 结 论

本文提出了一种基于 FPGA 的手机短信息加密系统, 该系统采用混沌序列作为初始密钥混合 A5/1 算法进行手机短信息的加密, 给出了具体的系统设计与硬件实现的方案. 详细介绍了混沌序列量化为二值的算法, 及混沌 A5/1 混合算法, 并在序列相关性测试理论中, 证明了圆周相关与线性相关的关系. 通过 SIM300 模块仿真普通手机功能, 保证普通短信息和加密短信息的正常传输. 本设计还开发了一套软件测试平台, 可以仿真两台手机进行短信息收发, 并与第三方的普通手机进行通信, 使硬件系统的测试结果清晰的展现在计算机上, 便于分析. 测试表明, 该系统实现了对短信息进行的安全加密和准确传输, 在保证手机短信息传输过程中的完整性和可靠性的同时, 提高了安全性, 实现了本设计的目的.

[1] Huang R S, Huang H 2005 *Chaos and its Applications* (2nd Ed.) (Wuhan: Wuhan University Press) p8 (in Chinese) [黄润生, 黄浩 2005 混沌及其应用 (第二版) (武汉: 武汉大学出版社) 第 8 页]

[2] Yu N, Ding Q, Chen H 2007 *J. Commun.* **28** 73 (in Chinese) [于娜, 丁群, 陈红 2007 通信学报 **28** 第 73 页]

[3] Li Q D, Yang X S 2007 *Acta Electron. Sin.* **35** 497 (in Chinese) [李清都, 杨晓松 2007 电子学报 **35** 497]

[4] Xu S J, Wang J Z 2008 *Acta Phys. Sin.* **57** 37 (in Chinese) [徐淑奖, 王继志 2008 物理学报 **57** 37]

[5] Xiang F, Qiu S S 2008 *Acta Phys. Sin.* **57** 6133 (in Chinese) [向菲, 丘水生 2008 物理学报 **57** 6133]

[6] Tong J G, Zhang Z X, Chen Z Q, Sun Q L 2011 *J. Harbin Eng. Univ.* **32** 760 (in Chinese) [佟吉钢, 张振新, 陈增强, 孙青林 2011 哈尔滨工程大学学报 **32** 760]

[7] Tang S, Chen H F, Hwang S K, Liu J M 2002 *Circuits and Systems-I, IEEE Trans.* **49** 163

[8] Zhou W J, Yu S M 2009 *Acta Phys. Sin.* **58** 113 (in Chinese) [周武杰, 禹思敏 物理学报 **58** 113]

[9] Zhang C X, Yu S M 2010 *Acta Phys. Sin.* **59** 3017 (in Chinese) [张朝霞, 禹思敏 2010 物理学报 **59** 3017]

[10] Jin J X, Qiu S S 2010 *Acta Phys. Sin.* **59** 792 (in Chinese) [晋建秀, 丘水生 2010 物理学报 **59** 792]

[11] Wu Y, Xiao J H, Wu Z Y, Yang J Z, Ma B J 2007 *Acta Phys. Sin.* **56** 2037 (in Chinese) [吴晔, 肖井华, 吴智远, 杨俊忠, 马宝军 2007 物理学报 **56** 2037]

[12] Hu G X 2007 *J. South-Central Univ. National.* (Nat. Sci. Edition) **26** 95 (in Chinese) [胡国香 2007 中南民族大学学报 (自然科学版) **26** 95]

[13] Chen Y T, Yang J Q, Kang R S, Ai Y L, Xie D L 2008 *Comput. Eng. Sci.* **30** 156 (in Chinese) [陈滟涛, 杨俊起, 康润生, 艾永乐, 谢东垒 2008 计算机工程与科学 **30** 156]

[14] May R M 1976 *Nature* **261** 459

[15] Wu H, Ding Q, Zhou P 2008 *Chin. J. Sci. Instrum.* **29** 372 (in Chinese)[巫红, 丁群, 周平 2008 仪器仪表学报 **29** 372]

[16] Callegari S, Dondini M, Setti G 2001 *Proc. IEEE Int. Symp. Circuits and Systems* ISCAS, March, 2001, 221–224

[17] Luo Q B, Zhang J 2006 *J. Electron. Inform. Tech.* **28** 1262 (in Chinese) [罗启斌, 张健 2006 电子与信息学报 **28** 1262]

[18] Farmer M E 2009 *Proc. 16th Int. Digital Signal Processing Conf.* p1–6

[19] Zhao Y X, Wang W, Liu L Q 2007 *Danjian Yu Zhidao Xue Bao* **27** 370 (in Chinese) [赵玉新, 王伟, 刘利强 2007 弹箭与制导学报 **27** 370]

[20] Qiu Y H, He C, Zhu H W 2002 *J. Shanghai Jiaotong Univ.* **36** 1788 (in Chinese) [邱跃洪, 何晨, 诸鸿文 2002 上海交通大学学报 **36** 1788]

[21] Ding Q, Wang L 2011 *Chin. J. Sci. Instrum.* **32** 2316 (in Chinese) [丁群, 王路 2011 仪器仪表学报 **32** 2316]

[22] Wang Y M, Liu J W 2003 *Security Theory and Technology of Communication Network* (Xi'an: Xidian University Press) (in Chinese) [王育民, 刘建伟 2003 通信网的安全理论与技术 (西安: 西安电子科技大学出版社)]

[23] Komninos N, Honary B, Darnell M 2002 *Proc. Third Int. 3G Mobile Communication Technologies Conf.* 2002 324–328

[24] Ahmad M, Izharuddin 2009 *Proc. Int. Multimedia, Signal Pro-*

cessing and Communication Technologies IMPACT '09. 2009 265–267

[25] Lau F C M, Tse C K 2003 *Chaos-Based Digital Communication Systems* (Berlin: Springer-Verlag)

[26] Chen W, Hu Y, Yang Y X, Niu X X 2006 *J. Electron. Inform. Tech.* **28** 827 (in Chinese) [陈伟, 胡云, 杨义先, 钮心忻 2006 电子与信息学报 **28** 827]

[27] Ding Q, Zhu Y, Zhang F Y, Peng X Y 2005 *Proceeding of ISCIT2005*. 2005 1009–1012

[28] Ding Q, Pan J, Wang L, Chen G R 2009 *International Workshop Chaos-Fractals Theories and Applications* (IWCFTA2009). November 19–21, 2009 143–147

[29] Qi N, Pan J, Ding Q 2011 *The First International Conference on Instrumentation and Measurement*, Computer, Communication and Control (IMCCC2011). October 22–25, 2011

Field programmable gate array-based chaotic encryption system design and hardware realization of cell phone short message*

Pan Jing Qi Na Xue Bing-Bing Ding Qun†

(*Electronic Engineering College of Heilongjiang University, Key Laboratory of Electronic Engineering College of Heilongjiang Province, Harbin* 150080*, China*)

(Received 8 December 2011; revised manuscript received 28 February 2012)

Abstract

More and more people having cell phone, they must pay more attention to message security of their personal privacy, in which cell phone short message security is the most important. In this paper, we focus on designing an encryption hardware system of cell phone short message with chaos and A5/1 hybrid algorithm and realizes it on field programmable gate array. In the encrypted core, chaotic sequences of logistic map are used as initial keys of A5/1 algorithm for encrypting short messages, and in this paper we prove the relationship between linear correlation and circle correlation in the pseudo-randomness research of chaotic sequences serving as the initial keys. The SIM300 modules are used to realize cell phone functions, simulate short messages of common cell phone and the encrypte short messages after processing by our system by wireless transmitting through the base station. In addition, in this paper we design a software test platform, and it can show the results of this hardware system on computer. The test results indicate that the proposed system and its hardware implementation can encrypt/decrypt short messages and ensure their normal transmission, which can improve the security of short message and ensure its integrity and reliability during transmitting.

Keywords: chaos and A5/1 algorithm, circle correlation, cell phone short message hardware encryption, software test platform

PACS: 05.45.Vx, 84.40.Ua, 43.38.Si

* Project supported by the National Natural Science Foundation of China (Grant No. 61072072), and the Students' Innovation Laboratory Project of Heilongjiang University, China (Grant No. CX11175).

† E-mail: qunding@yahoo.cn