面向 Android 的 RSA 算法优化与二维码加密防伪系统设计

方文和[1,2,3] 李国和[1,2,3] 吴卫江[1,2,3] 洪云峰[3] 周晓明[3]
(中国石油大学(北京)地球物理与信息工程学院 北京 102249)[1]
(中国石油大学(北京)油气数据挖掘北京市重点实验室 北京 102249)[2]
(石大兆信数字身份管理与物联网技术研究院 北京 100029)[3]

摘 要 面向 Android 智能手机终端,研究设计了移动二维码加密防伪系统,其加密模块基于 RSA 算法。为解决 RSA 算法在移动终端的运行效率问题,结合 Monte Carb 型概率算法与 Miller-Rabin 素数测试优化策略得到快速随机强素数算法以提高 RSA 算法的初始化及加密效率,并且采用 MMRC 解密算法来优化 RSA 解密过程,还引入了 M-ary 算法来对 RSA 算法过程中所进行的模幂运算进行优化计算。通过以上 3 个方面优化的实现,200 次对比实验表明,改进的 RSA 算法在 Android 加密防伪模块中的执行效率比原有算法有明显提升。

关键词 QR 码,RSA,Android,M-ary 算法,智能防伪
中图法分类号 TP399 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.01.034

Optimization of RSA Encryption Algorithm for Android Mobile Phone and Design of QR Code Encryption Security System

FANG Wen-he[1,2,3] LI Guo-he[1,2,3] WU Wei-jiang[1,2,3] HONG Yun-feng[3] ZHOU Xiao-ming[3]
(College of Geophysics and Information Engineering, China University of Petroleum, Beijing 102249, China)[1]
(Beijing Key Lab of Data Mining for Petroleum Data, China University of Petroleum, Beijing 102249, China)[2]
(PanPass Institute of Digital Identification Management and Internet of Things, Beijing 100029, China)[3]

Abstract Based on the Android intelligent mobile terminal, the mobile two-dimensional code encryption security system was designed. The encryption module is based on RSA algorithm. To improve the running efficiency of RSA algorithm in the mobile terminal, the Monte Carb probabilistic algorithm is combined with Miller-Rabin prime test optimization strategies to get rapid random strong prime algorithm to improve the RSA algorithm efficiency of initialization and encryption, and MMRC decryption algorithm was used to optimize RSA decryption process. In addition, the M-ary algorithm was introduced to optimize the modular exponentiation carried out during the RSA algorithm. By realizing the above three aspects of optimazation, the 200 comparison test results show the improved RSA algorithm has improved significantly in the Android cryptographic security module than the original RSA algorithm.

Keywords QR code, RSA, Android, M-ary algorithm, Smart security

加密算法的执行效率和安全性是加密防伪技术研究关注的两大重点,安全性提升往往以牺牲算法执行效率为代价。RSA 算法的安全性依赖于大数分解,安全性高,应用范围广[1]。由于 RSA 算法计算模正整数次幂时计算量巨大,降低了 RSA 算法的执行效率[9]。目前多采用高速模乘[4]、DSP 芯片[15]、PC 并行计算[18]以及将其中幂剩余变成一系列平方剩余和乘同余的迭代[10]等方式来提高传统 RSA 算法的效率。

而这些 PC 上的传统方式在 Android 智能手机终端上不太适用,传统的 RSA 算法在手机客户端上的执行效率低下,导致用户体验差、等待时间长等问题,使得 RSA 算法在 Android 移动手机客户终端的应用受到很大限制。二维码防伪实际查询需要较快的响应速度。由于安全性要求用户选择的素数多为 100 位左右的十进制数[25],安全性的关键即是该素数位数长度,在该长度素数安全性要求下,标准的 RSA 算法加解密速度缓慢,效率低下,难以满足 Android 手机客户端的用户体验需求,使得实际应用非常受限。

因此,本文面向 Android 智能手机终端设计移动二维码加密防伪系统,其加密模块基于 RSA 算法,为解决 RSA 算法在移动终端的运算效率问题,结合 Monte Carb 型[1]概率算法与 Miller-Rabin 素数测试优化策略[10]得到快速随机强素数算法以提高 RSA 算法初始化及加密效率,并采用 MMRC[8]解密算法优化 RSA 解密过程,还引入了 M-ary 算法[20]对 RSA 算法过程中 $C=M^e \bmod N$[4]所进行的模幂运算进行快速优化计算。以上 3 个方面的优化措施在Android平台编码

到稿日期:2015-12-14 返修日期:2016-03-28 本文受国家高新技术研究发展计划(2009AA062802),国家自然科学基金(60473125),中国石油(CNPC)石油科技中青年创新基金(05E7013),国家重大专项子课题(G5800-08-ZS-WX)资助。
方文和(1991—),男,硕士生,主要研究领域为知识发现、数据挖掘、信息安全;李国和(1965—),男,博士,教授,博士生导师,主要研究领域为人工智能、知识发现、信息安全;吴卫江(1971—),男,博士生,副教授,主要研究领域为人工智能、知识发现;洪云峰(1966—),男,主要研究领域为 ERP 与数据管理;周晓明(1963—),男,工程师,主要研究领域为信息管理系统、决策支持,E-mail:710911939@qq.com。

实现，使得 RSA 加解密模块在 Android 手机防伪模块中的执行效率更高。对于密钥模值长度为 512 位、1024 位、2048 位这 3 种代表性长度（安全性等级：生活安全度、商务安全度、机密安全度），各经过 200 次的对比实验表明，Android 加密防伪效率比原有算法有明显提升。

1　二维码与防伪技术

二维码于平面二维方向上表达信息[11]。与一维码单维度相比，它能够表达的信息量更大，也适合表达复杂的文字信息，其内部结构复杂，空间利用率高，纠错能力强[17]。由于其复杂的内部结构，很难对生成后的二维码进行修改，使得其更具安全性[26]。

QR Code 的全称为“快速响应矩阵码”，其结构如图 1 所示，是一种高效的矩阵式二维码符号[17]。

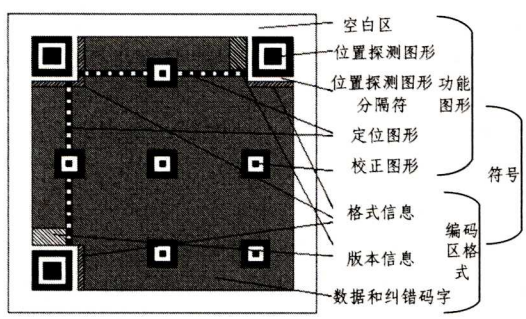

图 1　QR 码结构

与其他码制的二维码相比，QR 码具有以下特点[11]：1）超高速识读；2）全方位识读；3）纠错能力强；4）能够更高效地表示汉字。

加密 QR 码防伪技术利用加密算法实现二维码加密，只有专门的软件或者通过专门的验证服务器才能识别查询。加密 QR 码防伪技术有信息容量大、安全性高、可追踪性强、可读性强、纠错性能强、抗损性强、占用空间小、使用寿命长、成本低等一系列优势[11]。可以通过手机智能终端轻松识别，而且在防伪的同时还可以利用二维码信息量大的特点，加入相关信息，实现公司及产品的推广，建立消费者与企业沟通的安全信任渠道以及产品溯源体系。

2　加密算法设计改进

2.1　RSA 算法

1978 年美国麻省理工学院的 3 位教授 R. L. Rivest，A. Shamir 和 M. Adleman 提出了一种基于因子分解的指数函数[2]作为单向陷门函数[3]的公开密钥密码算法（PKC），即著名的 RSA 算法[4]。RSA 算法基于一个简单的数论事实：将两个大素数相乘十分容易，但是若要对其乘积进行因式分解却极其困难，因此可以将乘积公开作为加密密钥[5]。

标准的 RSA 算法描述如下。

（1）随机选择不相同且充分大的素数 p,q。

（2）计算 $n=p*q$。

（3）计算 Euler 函数 $f(n)=(p-1)(q-1)$，将 n 公开，同时对 $p,q,f(n)$ 严加保密，此时 $f(n)$ 的值计算问题是 NP 问题。

（4）随机抽取与 $f(n)$ 互质的正整数 e，$gcd(e,f(n))=1$，同时满足：$1<e<f(n)$。

（5）根据扩展 Eulicd 算法[6]计算 $d=e^{-1}(\mathrm{mod}\ f(n))$，即计算 d，使得 $d*e\equiv 1\mathrm{mod}\ f(n)$。

（6）公钥 $KU=(e,n)$，私钥 $KR=(d,n)$。密钥空间：$K=\{(n,p,q,e,d)\}\mid n=pq$，$p$ 与 q 为不同大素数，$ed=1(\mathrm{mod}\ f(n))$。RSA 算法中 $F(x)=x^t(\mathrm{mod}\ n)$（其中 $t\in K$ 且 $x\in Z_n$）。

得到公钥 $KU=(e,n)$，私钥 $KR=(d,n)$ 后，对信息进行加解密的过程描述如下。

（1）加密。先将明文信息变换成 0 至 $n-1$ 的整数 M。设密文为 C，则 $C=E_{KU}(M)=M^e(\mathrm{mod}\ n)$，其中 $1\leqslant M\leqslant n-1$ 为明文。

（2）解密。解密运算定义为：$M=D_{KR}(c)=c^d(\mathrm{mod}\ n)$，其中 $1\leqslant c\leqslant n-1$ 为密文。

RSA 算法的实现流程如图 2 所示。

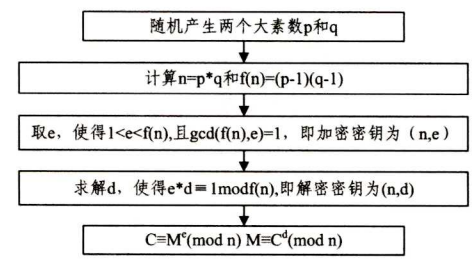

图 2　RSA 算法实现流程图

2.2　随机强素数快速生成

定义 1　令 x 为不小于 1 的正整数，p 设定为素数，称 $\pi(x)=\sum_{p\leqslant x}1$ 为素数的分布规律函数。$\pi(x)$ 是小于等于 x 的全部素数的个数，对 $\pi(x)$ 的渐进性进行研究[7]，可得如下素数定理。该定理涉及到复分析、黎曼 ζ 函数。黎曼 ζ 函数与 $\pi(x)$ 关系密切[18]。

定理 1　素数分布规律函数 $\pi(x)$ 是 $\frac{x}{\ln x}$ 的渐进，即 $\lim\limits_{x\to\infty}\frac{\pi(x)\ln x}{x}=1$。由定理 1 可知，当 x 足够大时，$\pi(x)\approx\frac{x}{\ln x}$[8]。

定理 2　大于 1 的正整数 n 是素数的充分必要条件为：$(x+1)^n\equiv(x^n+1)(\mathrm{mod}\ n)$[8]。其在正整数系数多项式集合 $Z[x]$ 中成立。由于 $Z[x]$ 是环，因此 $(x+1)^n\equiv(x^n+1)(\mathrm{mod}\ n)$ 也可表示为：$(x+1)^n-(x^n+1)=nq(x)$，$q(x)\in Z[x]$。

RSA 算法涉及到随机强素的生成，其效率影响到 RSA 算法的初始化和加密效率。强素数的产生方法包括确定性迭代生成素数算法，如 Demytko 算法[7]；另一种方法是先快速随机生成一个大素数，再通过概率算法检测，如 Lehmann 算法和 RabinMiller 算法[7,8]。

正整数序列中散布的素数非常不规则，还没有公式可以直接计算出一个特定长度的大素数。通过迭代算法生成的素数缺少随机性，不适合用来进行 RSA 算法的加密改进[9]。概率算法为时间多项算法，快速简便，故适合用来进行 RSA 算法的加密改进，其采用了快速随机生成强素数的思路。

常见的素数检测方法有 Miller-Rabin 检测[10]、Solovay-Stassen 检测法和 Lehman 检测法。

根据 Monte Carb 型概率算法，联合 Miller-Rabin[9]素数检测优化策略可以得到大素数快速生成算法，如图 3 所示。

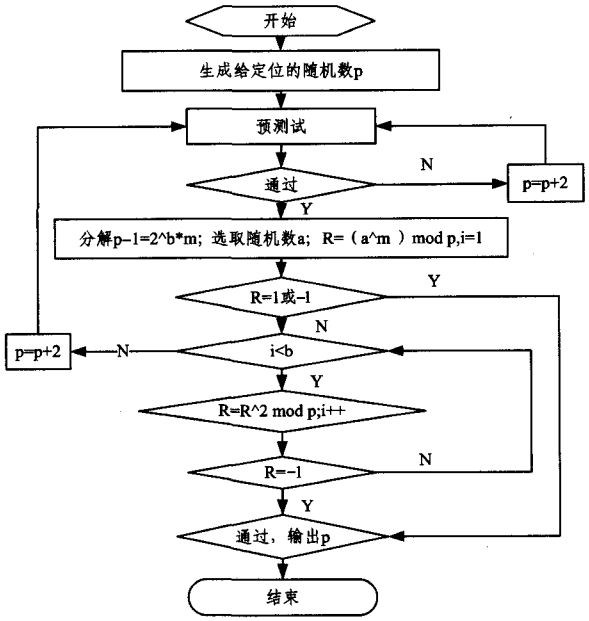

图 3 快速随机大素数检测生成算法流程图

把需要检测的数记为 p，求算 b(b 是 2 整除 $p-1$ 的最大次数)。随后根据 $p=1+2^b\times m$ 计算求得 m 进入检测。检测算法如下。

(1)输入：一个小于 p 且大于 1 的随机素 a。输出：p 是素数或 p 不是素数。

(2)设 $j=0$，计算 $z=a^m \pmod p$。

(3)如果 z 与 1 或 $p-1$ 同余，则 p 通过检测，可能是素数。

(4)如果 $j>0$ 且 $z=1$，则 p 不是素数。

(5)令 $j=j+1$，若 $j<b$ 且 z 与 $p-1$ 不同余，则计算 $z=z^2 \pmod p$，然后返回步骤(4)。如果 z 与 $p-1$ 同余，则 p 通过检测，可能是素数。

(6)若 $j=b$ 且 z 与 $p-1$ 不同余，则 p 不是素数。

(7)退出。

该算法为多项式的时间算法，具有较高的执行效率，如果被检测的数通过 t 次检测时被检测数不是素数的概率不会大于 $\frac{1}{4^t}$，当通过检测的次数 t 充分大时，n 为非素数是一个小概率事件，这时其算法时间复杂度为 $O((\log_2 n)^3)$，近似于 Solovag-Strassen 算法[7]，其每次检测过程中的误判率不到 $\frac{1}{4}$。

2.3 中国剩余定理推导及算法改进

2.3.1 中国剩余定理

$m_1,m_2,\cdots,m_r$ 两两互为素数的正整数，$a_1,a_2,\cdots,a_r$ 为整数，故同余方程组 $x\equiv a_i \pmod{m_i}(i=1,2,\cdots,r)$，模 $M=m_1m_2\cdots m_r$，其唯一解 $x=\sum_{i=1}^{r}a_iM_iy_i \bmod M$，其中 $M_i=\frac{M}{m_i}$，$y_i=M_i^{-1} \bmod m_i(i=1,2,\cdots,r)$。

其解有两种方法：单基数转换法(Single-Radex Conversion，SRC)和混合技术转换法(Mixed-Radex Conversion，MRC)[4]。

2.3.2 CRT 定理改进 RSA 算法

算法 1 CRT 的单基数转化法(SRC)

1. 计算 $P\leftarrow p_1p_2\cdots p_s$ 和 $P_i\leftarrow P/p_i 1\leqslant i\leqslant s$；
2. 计算 $Q_i\leftarrow P_i^{-1} \pmod{p_i}(1\leqslant i\leqslant s)$；
3. 计算唯一解 $x\leftarrow d_1P_1Q_1+d_2P_2Q_2+\cdots+d_sP_sQ_s \pmod P$。

该方法由 H. L. Garner 于 1958 年首先提出。之后 D. E. Kunth 将其用于计算数论，并进行了有益的改进[4]。经 Kunth 改进后的 MRC 方法如算法 2 所述。

算法 2 CRT 的混合基数转换法(MRC)

1. 计算 $B_{ji}\leftarrow p_j \pmod{p_i},1\leqslant j<i\leqslant s$。
2. 分别计算：

$v_1\leftarrow d_1 (\mathrm{mod} p_i)$；

$v_2\leftarrow (d_2-v_1)B_{12} \pmod{p_2}$；

…

$v_s\leftarrow (d_s-(v_1+p_1(v_2+p_2(v_3+\cdots+p_{s-2}v_{s-1})\cdots)))B_{1s}B_{2s}\cdots B_{(s-1)s} \pmod{p_s}$

3. 求唯一解 $X\leftarrow v_sp_{s-1}\cdots p_2p_1+\cdots+v_3p_2p_1+v_2p_1+v_1$。

将其解密运算过程从模 n 的指数型转变为求解同余方程组的型式。

定理 3(CRT 推论)[12] 令 $p_1,p_2,\cdots,p_s$ 两两互为素数的正整数，$P=p_1p_2\cdots p_s$，则 $f(x)\equiv 0 \pmod P$ 与 $f(x)\equiv 0 \pmod{p_i}(1\leqslant i\leqslant s)$ 等价。

定理 4(费马小定理)[12] p 为素数，x 为满足 $x \pmod p\neq 0$ 条件的整数，则：

$$x^{p-1}\equiv 1 \pmod p$$

由算法 1 和算法 2，RSA 的解密算法 $m=D_{KR}(c)=c^d \pmod n$，由于拥有私钥 $KR=(d,n)$ 的合法用户已知 $n=pq$(p 和 q 为不同的素数)，因此由定理 3，把 RSA 的解密由计算模 n 的指数运算 $m=D_{sk}(c)=c^d \pmod n$ 推导转变为计算模 p 和模 q 的同余式方程组：

$$\begin{cases} m_1\equiv c^d \pmod p \\ m_2\equiv c^d \pmod q \end{cases} \tag{1}$$

由定理 4 及同余式 $m_1=c^d \pmod p$：令 $r=d \pmod{p-1}$，则存在 k 满足：$d=k(p-1)+r$。故：

$$\begin{aligned} m_1=c^d \pmod p &\equiv c^{k(p-1)+r} \pmod p \equiv c^{k(p-1)}c^r \pmod p \\ &\equiv (c^{(p-1)} \bmod p)^k c^r \pmod p \equiv 1^k c^r \pmod p \\ &\equiv c^{d \bmod (p-1)} \pmod p \\ &\equiv (c \bmod p)^{d \bmod (p-1)} \pmod p \end{aligned}$$

同理，对同余式 $m_2\equiv c^d \pmod q$，有：

$$m_2\equiv c^d \pmod q \equiv c^{d \bmod (q-1)} \pmod q \equiv (c \bmod q)^{d \bmod (q-1)} \pmod q$$

最终，同余式方程组(1)转化为：

$$\begin{cases} m_1\equiv (c \bmod p)^{d_1} \pmod p \\ m_2\equiv (c \bmod q)^{d_2} \pmod q \end{cases} \tag{2}$$

其中，$d_1=d \pmod{p-1}$，$d_2=d \pmod{q-1}$。

故其解密运算与余式方程组(2)相同。由算法 1 对其求解，即是如下的快速 RSA 解密算法。

算法 3 RSA 的 SRC 解密算法

1. 计算 $d_1\leftarrow d \pmod{p-1}$ 与 $d_2\leftarrow d \pmod{q-1}$；
2. 计算 $C_1\leftarrow c \pmod p$ 与 $C_2\leftarrow c \pmod q$；
3. 计算 $M_1\leftarrow C_1^{d_1} \pmod p$ 与 $M_2\leftarrow C_2^{d_2} \pmod q$；
4. 计算 $B_1\leftarrow q^{-1} \pmod p$ 与 $B_2\leftarrow p^{-1} \pmod q$；
5. 计算 $m\leftarrow M_1B_1q+M_2B_2p \pmod N$。

通过算法 2 求解方程组(2)，构造三角形数值表：

M_{11}

M_{21} M_{22}

其中：

$M_{11}=m_1, M_{21}=m_2$

$M_{22}=(M_{21}-M_{11})(p^{-1} \bmod q)(\bmod q)$

$=(m_2-m_1)(p^{-1} \bmod q)(\bmod q)$

再由算法 2 得到：

$m=m_1+[(m_2-m_1)(p^{-1} \bmod q)(\bmod q)] * p$

由此得到如下的快速 RSA 解密计算算法。

算法 4　RSA 的 MMRC 解密算法

1. 计算 $d_1 \leftarrow d(\bmod p-1)$ 与 $d_2 \leftarrow d(\bmod q-1)$；
2. 计算 $C_1 \leftarrow c(\bmod p)$ 与 $C_2 \leftarrow c(\bmod q)$；
3. 计算 $M_1 \leftarrow C_1^{d_1}(\bmod p)$ 与 $M_2 \leftarrow C_2^{d_2}(\bmod q)$；
4. 计算 $B \leftarrow p^{-1}(\bmod p)$；
5. 计算 $m \leftarrow M_1+[(M_2-M_1) * B(\bmod q)] * p$。

因为算法 3 与算法 4 的前 3 个步骤完全相同，运算量相当，所以比较它们的后两个步骤。对于算法 3，计算量包括逆元 2 次、加法 1 次和 2k 比特模余 1 次；而对于算法 4，计算量包括逆元 1 次、乘法 2 次、加法 1 次、减法 1 次和 k 比特模余 1 次。忽略加减法运算量。显然，从理论上比较来看，算法 4 的后面两个步骤的运算量比算法 3 后面两个步骤的少一半，故效率进一步提升。

2.4　M-ary 算法

模幂运算的研究对象：假设 N, M, e 都为 k 个二进制位的大整数，k 很大（$k>256$）时，快速计算[18]：

$$C=M^e \bmod N \tag{3}$$

该式一般转化为一系列的模乘和模平方计算，即如下形式：

$$M \rightarrow M^2 \rightarrow M^3 \rightarrow \cdots \rightarrow M^e$$

从左到右扫描指数，假设指数 e 按式(4)表示：

$$e=(e_{k-1}e_{k-2}\cdots e_1 e_0)=\sum_{i=0}^{k-1} e_i 2^i (e_i \in \{0,1\}) \tag{4}$$

M-ary 算法[13]实际上是二元法的推广，该方法首先把式(4)的指数按 d 位为单元分成 s 块，不足 d 位的在高位补 0，以满足 $sd=k$。定义：

$$F_i=(e_{id}+(d-1)e_{id}+(d-2)e_{id}+\cdots e_{id}) \tag{5}$$

则在新基下的指数 e 可表示为：

$$e=\sum_{i=0}^{s-1} F_i 2^{id} (0 \leqslant F_i \leqslant m-1), m=2^d$$

该算法的思路为先计算出 $M^\omega \bmod N(\omega=2,3,4,\cdots,m-1)$ 的值，然后以 d 位为单位从高位到低位扫描指数 e，每次循环都对中间结果求 2^d 幂以及求与 M^{F_i} 模乘。该算法如下。

Input：N，M，e

Output：$C=M^e \bmod N$

1. 计算并存储 $M^e \bmod N, \omega=2,3,4,\cdots,m-1$；
2. 以 d 位为单元重新表示 e，共 s 位；
3. $C: M_{s-1}^F \bmod N$；
4. For i：=s−2 down to 0；
5. $C: C^{2d} \bmod N$；
6. If $F_i \neq 0$ then $C: C \times M^{F_i} \bmod N$；
7. Return C。

3　系统设计及实验结果分析

3.1　系统设计

3.1.1　开发与运行环境

手机客户端软件采用 Eclipse 工具下的 Android 插件进行开发，Android API 等级为 15，即 Android 4.0.3，程序设计基于 Java 语言和 C 语言实现。Android NDK 版本为 r9d，使用 Cygwin 模拟 Linux 编译环境。

服务端系统基于.NET 平台开发，采用 C# 语言，运行环境为 Windows Server 2003，IIS 版本为 IIS6.0。

3.1.2　服务平台架构设计

防伪数码的验证服务支持消费者用户通过电脑网页、移动手机应用、短信、微信公众号等不同方式进行验证。因此防伪平台架构设计如图 4 所示，基于 B/S 架构设计开发，系统实现采用 4 层架构：显示层（UI）、服务层（Service）、业务逻辑层（BLL）和数据访问层（DAL）；主要事务逻辑在服务端（SERVER）实现，任何一个应用从逻辑上都可以划分为用户界面逻辑、应用处理逻辑和数据逻辑。网站、移动端、第三方应用等通过 Web Service 接口对防伪查询服务进行调用。

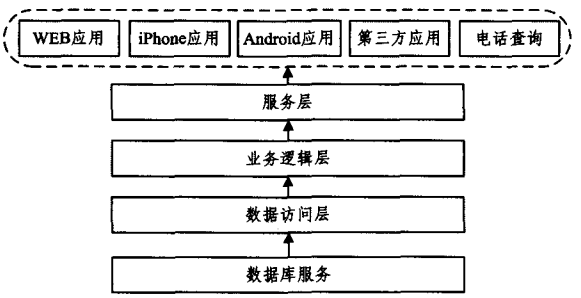

图 4　防伪平台架构

3.1.3　加解密系统模块设计

防伪数码在打印至标签之前，在服务端使用加密密钥对整个批次的数码进行加密处理生成密文，在消费者使用移动端扫码时才会对密文进行解密，总体加密防伪系统的模块结构如图 5 所示。

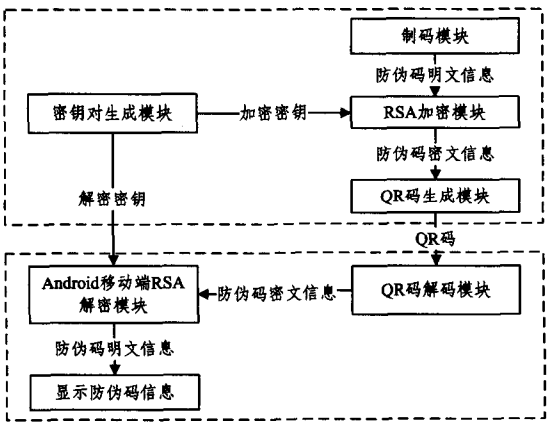

图 5　加解密系统模块结构图

（1）制码模块：每一件商品从生产开始都会分配一个唯一的防伪编码。根据编码规则，生成 16 位的十进制序列号，在系统中与所属的产品类型、批次等基本信息进行关联，并标明是否已经启用。

（2）密钥对生成模块：通过 RSA 密钥生成算法，设置将生成的密钥的模值长度，产生密钥对，将其加密密钥应用于防伪系统中的防伪码加密模块，将解密密钥嵌入到防伪系统移动端的识读软件中，对二维码信息进行解密。

（3）RSA 加密模块：不直接使用防伪序列号生成二维码，而是利用加密密钥对明码信息进行加密后得到一串没有规律的字符串再生成二维码。

（4）QR 码生成模块：根据 QR 码的编码规则，将字符串

信息编码生成 QR 码，然后再打印。

(5)QR 码解码模块：它为 QR 编码的逆过程，解码后得到防伪码的密文信息。

(6)移动端 RSA 解密模块：把密文信息转化还原成明文的十进制防伪数码。

3.1.4 二维码识别与数码解密

数码验证功能包括二维码扫描、二维码解码、密文解密、结果显示 4 个步骤，其流程如图 6 所示。

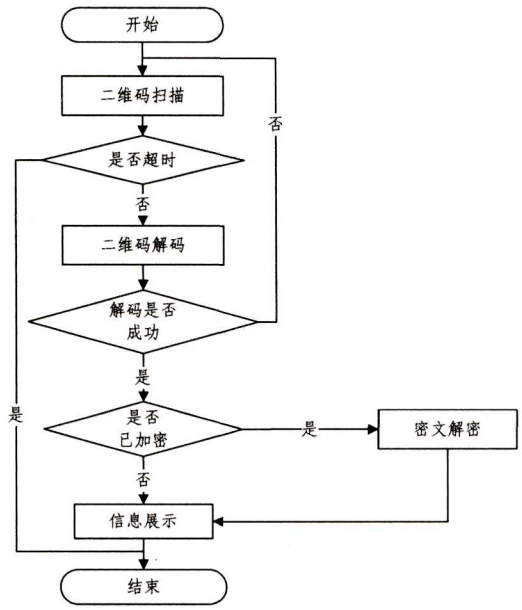

图 6 QR 解码及密文解密流程图

为提高二维码的识别效率，摄像头预览界面以交互形式绘制矩形框以减小条码区域定位范围。初始化相机参数，实例化自定义的类 DrawRect. java，其继承自 View 类，以屏幕为画布，重载 onDraw 函数，绘制标签拍摄预览的矩形框，过程如下：

1)获取屏幕分辨率，根据分辨率设置矩形框的大小；

2)实例化 Paint 对象，并设置画笔颜色；

3)调用 canvas. drawRect()方法在屏幕上边缘绘制 4 个矩形，留下屏幕中间矩形预览数字标签。

将预览图像分配给子线程处理，其中二维码解码算法采用条码识别库 ZXing，解码成功后判断是否为加密信息，若为加密信息，则利用嵌入到移动端软件的 RSA 解密密钥对密文进行解密，得到明文的防伪码信息后，跳转页面，将解码的图像以及识别结果显示出来，给出鉴定数码真伪信息的说明。

3.2 实验对比结果

实验采用 Android 智能手机对 QR 码进行扫描识别，实验环境的参数为：操作系统版本为 4. 0. 4，CPU 为高通骁龙 Snapdragon MSM8260，主频为 1741MHz，内存为 1GB，摄像头为 800 万像素，支持自动对焦。

分别利用标准的 RSA 算法与改进后的 RSA 算法在该模块下进行测试。采用 OpenSSL 生成 RSA 密钥对，利用加密密钥对商品防伪数码“0044669511201239”进行加密生成密文信息，并将密文信息生成 QR 码，图 7 示出了密钥的模值长度为 512 位、1024 位、2048 位时标准的 RSA 与改进后 RSA 的加密密文编码结果。

(a)模值长度为 512 位 (b)模值长度为 1024 位 (c)模值长度为 2048 位

图 7 密文 QR 码

分别采用标准 RSA 解密算法和改进的 RSA 解密算法对密钥模值长度为 512 位、1024 位、2048 位的密文字符串进行加密，对每一种密钥长度进行 200 次实验，测试加密模块对密文字符串进行加密所需要的时间，统计结果如表 1 所列。随着 RSA 密钥长度的增加，加密效率急剧下降，不过改进后的 RSA 算法加密所用的时间少，效率高。

表 1 加密速度测试结果

密钥长度(位)	标准算法平均时间(ms)	改进 RSA 算法平均时间(ms)
512	15.64	5.75
1024	34.42	12.23
2048	87.26	23.83

分别采用标准 RSA 解密算法和改进的 RSA 解密算法对密钥模值长度为 512 位、1024 位、2048 位时的密文字符串进行解密，对每一种密钥长度分别进行 200 次实验，测试解码模块对密文字符串进行解密所需要的时间，统计结果如表 2、图 8 所示。

表 2 解密速度测试结果

密钥长度(位)	标准算法平均时间(ms)	改进 RSA 算法平均时间(ms)
512	8.64	1.75
1024	23.42	5.23
2048	53.26	12.83

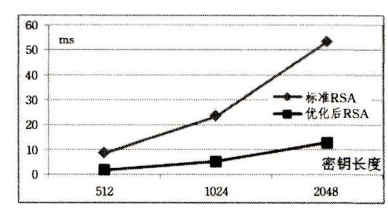

图 8 解密速度测试结果对比

采用标准 RSA 解密算法对其进行扫描解码，当密钥长度不大于 512 位时，移动客户端能够迅速实现 QR 码的识别；当密钥长度为 1024 位时，识别成功率下降，对摄像头的对焦参数要求较高，需要在支持近距离对焦摄像且长时间等待的条件下才能识别成功；采用 2048 位的密钥时，基本无法实时对二维码信息进行解码。

采用改进的 RSA 解密算法对其进行扫描解码，解密速度明显更快，当密钥长度不大于 512 位时，移动客户端能够非常迅速地实现 QR 码的识别；当密钥长度为 1024 位时，解密速度稍微下降；采用 2048 位的密钥时，对二维码信息进行解码的速度开始明显下降。

经过 200 次对比实验得出结论：采用 3 个方面的优化措施后，在 Android 平台编码实现的 RSA 改进模块使得其在 Android 平台应用中的执行效率比标准库 RSA 算法更高。Android 加密防伪效率比原来有明显提升，使得在 Android 手机防伪模块中的执行效率更高。

结束语　本文面向 Android 智能手机终端设计了移动二维码加密防伪系统，其加密模块基于 RSA 算法，为解决 RSA 算法在移动终端的运算效率问题，将 Monte Carb 型概率算法结合 Miller-Rabin 素数测试优化策略得到快速随机强素数算法，以提高 RSA 算法初始化及加密效率；并且采用 MMRC 解密算法优化 RSA 解密过程，还引入了 M-ary 算法对 RSA 算法过程中所进行的模幂运算进行快速优化计算。通过以上 3 个方面的优化实现，200 次对比实验表明在该 Android 数字防伪平台下，随着 RSA 规模的增大，标准库 RSA 算法加解密速度明显下降。而利用优化的 RSA 算法实现的模块系统执行效率明显提高，使得其在 Android 手机防伪模块中的执行效率更高。

参 考 文 献

[1] MA Chang-sha, HU Ai-qun. Research on improving the speed of RSA algorithm [J]. Information Security and Communications Privacy, 2010(10): 80-82. (in Chinese)
麻常莎，胡爱群. 关于提高 RSA 算法速度的研究[J]. 信息安全与通信保密，2010(10)：80-82.

[2] RIVEST R L, SHAMIR A, ADLEMAN M. A Method for Obtaining Digital Signnature and Public-key Cryptosystems [J]. Communication of the ACM, 1978, 21(2): 120-126.

[3] DIFFIE W, HELLMAN M E. New Direction in Cryptography [J]. IEEE Transaction on Information Theory, 1976, IT-22(6): 644-654.

[4] HE Yi-chao, LIU Jian-qin, HEN Wei-hai. The Chinese remainder theorem in the application of the RSA decryption[J]. Journal of Hebei Academy of Sciences, 2003(3): 138-143. (in Chinese)
贺毅朝，刘建芹，陈维海. 中国剩余定理在 RSA 解密中的应用[J]. 河北省科学院学报，2003(3)：138-143.

[5] XIAO Ping, LI Xi. Based on RSA digital envelopes technology Android data security mechanism[J]. Information Network Security, 2013(3): 37-39. (in Chinese)
肖萍，李茜. 基于 RSA 数字信封技术的 Android 数据安全机制[J]. 信息网络安全，2013(3)：37-39.

[6] KNUTH D E. The Art of Computer Programmings: Seminumerical Algorithms[M]. Stanford University, 2004

[7] FENG Deng-guo, FEI Ding-yi. Cryptography guidance[M]. Beijing: Science press, 2001. (in Chinese)
冯登国，裴定一. 密码学导引[M]. 北京：科学出版社，2001.

[8] 密码编码学与网络安全-原理与实践[M]. 刘玉珍，等译. 北京：电子工业出版社，2004.

[9] WANG Ying. RSA algorithm quickly generate method of large prime Numbers[J]. Journal of Hunan Institute of Science and Technology, 2005(5): 14-16. (in Chinese)
王英. RSA 算法中大素数的快速生成方法[J]. 湖南科技学院学报，2005(5)：14-16.

[10] HE Yi-chao, LIU Kun-qi. Rapid Realization of Rabin cipher[J]. Application Research of Computers, 2006, 23(9): 51-53. (in Chinese)
贺毅朝，刘坤起. Rabin 密码算法的快速实现研究[J]. 计算机应用研究，2006，23(9)：51-53.

[11] FANG Yuan, FU Hua-ming. Two-dimensional bar code encryption algorithm research[J]. Electronic-technique, 2009(1): 50-51. (in Chinese)
方媛，傅华明. 二维条码加密算法的研究[J]. 电子技术，2009(1)：50-51.

[12] ROSE K H. Elementary Number Theory and Its Application [M]. Addison-Wesley, 1984.

[13] KOC C K, Hung C Y. Adaptive M-ary Segmentation and Canonical Recoding Algorithms for Multiplication of Large Binary Numbers[J]. Computers and Mathematics with Applications, 1992, 24(3): 3-12.

[14] DOWNEYP, LEONYB, SETHIR. Computing Sequence with Addition Chains[J]. SIAM Journal of Computing, 1981, 10(3): 638-646.

[15] RAO jin-ping, FENG Deng-guo. Research and implementation of high speed RSA processing chip[J]. Computer Engineering and Applications, 2003(5): 139-141. (in Chinese)
饶进平，冯登国. 高速 RSA 处理芯片的研究与实现[J]. 计算机工程与应用，2003(5)：139-141.

[16] WANG Hao, OU Yan-ming. 2D-Bar codes reading: solutions for camera phones[J]. International Journal of Signal Processing, 2006, 3(3): 164-170.

[17] State Bureau of Quality Supervision. GB/T 18284-2000, quick response code[S]. Beijing: Beijing Standard Press, 2001. (in Chinese)
国家质量监督局. GB/T 18284－2000，快速响应矩阵码[S]. 北京：北京标准出版社，2001.

[18] ALSUWAIYEL M H. Algorithm Design Techniques and Analysis(English Version) [M]. Beijing: Electronic Industry Press, 2003.

[19] LIU Jian, SUN Ke-qin, WANG Sun-lv. Control flow analysis based on the Android system code vulnerability mining[J]. Journal of Tsinghua University (Natural Science Edition), 2012(10): 1335-1339. (in Chinese)
刘剑，孙可钦，汪孙律. 基于控制流挖掘的 Android 系统代码漏洞分析[J]. 清华大学学报(自然科学版)，2012(10)：1335-1339.

[20] SUN Run-kang, ZHANG Xian, SHAO Yu-ru, et al. Android phone security detection and forensic analysis system[J]. Information Network Security, 2013(3): 71-74. (in Chinese)
孙润康，展娴，邵玉如，等. Android 手机安全检测与取证分析系统[J]. 信息网络安全，2013(3)：71-74.

[21] LIU Xiao-ming. Construction of two dimensional code anti fake system with asymmetric encryption[J]. Software Guide, 2015(3): 145-151. (in Chinese)
刘小铭. 非对称加密二维码防伪系统构建[J]. 软件导刊，2015(3)：145-151.

[22] ZHOU Ze-yun, XIANG Yang-xia, ZOU Yu. Application of Android system in equipment support information system [J]. Sichuan ordnance Journal, 2015(4): 77-80. (in Chinese)
周泽云，向阳霞，邹渝. Android 系统在装备保障信息系统中的应用[J]. 四川兵工学报，2015(4)：77-80.

[23] ZHOU Xiao-qing, LU Tao, JIAO Qiang. Anti counterfeiting system based on QR code [J]. Computer and Modern, 2015(1): 122-126. (in Chinese)
周晓庆，陆涛，焦强. 基于 QR 码的药品防伪系统[J]. 计算机与现代化，2015(1)：122-126.

[24] LIN Yong, LU Jiang-hai, YAO Jun. Construction of two dimensional code inspection report anti fake platform based on RSA digital signature [J]. Quality and Technical Supervision Research, 2015(4): 55-57. (in Chinese)
林涌，卢江海，姚军. 基于 RSA 数字签名的二维码检验报告防伪

平台构建[J]. 质量技术监督研究,2015(4):55-57.

[25] WU Kai. The design and implementation of bar code scanning software based on Android platform[J]. Information Safety, 2013(10):223-231. (in Chinese)
吴凯. 基于 Android 平台的条码扫描软件的设计与实现[J]. 信息安全,2013(10):223-231.

[26] XU Jie-min, XIAO Yun. The present situation and development prospect of two dimensional bar code technology [J]. Computer and Modernization, 2004(12):141-142. (in Chinese)
徐杰民,肖云. 二维条码技术现状及发展前景[J]. 计算机与现代化,2004(12):141-142.

[27] ZHANG Xiao. Research and implementation of software protection strategy based on Android platform[D]. Beijing: Beijing University of Posts and Telecommunications, 2015. (in Chinese)
张晓. 基于 Android 平台的软件保护策略的研究与实现[D]. 北京:北京邮电大学,2015.

[28] LIU Zhi. Application of three weight DES, RSA, SHA-1 algorithm design data encryption system[J]. Software Guide, 2015 (5):165-167. (in Chinese)
刘志. 应用三重 DES、RSA、SHA-1 算法设计数据加密系统[J]. 软件导刊,2015(5):165-167.

[29] CHENG Xiao-rong, MA Li, HE Zhuang-zhuang. Analysis and improvement of public key RSA encryption algorithm[J]. Network Security, 2015(8):44-45. (in Chinese)
程晓荣,马力,何壮壮. 公钥 RSA 加密算法的分析与改进[J]. 网络安全,2015(8):44-45.

(上接第 158 页)

对存储资源的需求,提高了协议的扩展性。

表 3 加密操作对比

	Protocol	2C	2S	Total
Our	Signing/private key decryption	3	4	7
	Verifying/public key encryption	3	4	7
	Symmetric key encryption/ decryption	2	1	3
Chen L[13]	Signing/public key decryption	0	2	2
	Verifying/public key encryption	2	0	2
	Symmetric key encryption/ decryption	2	2	4

结束语 本文提出了一种新的基于 PKI 体系的跨域密钥协商协议,采用公钥算法与 Diffie-Hellman 协议协商得到安全会话密钥,解决了基于口令的跨域密钥协商协议和 Kerberos 协议存在的弱口令的安全问题。本协议共享密钥仅仅作为鉴别用户身份的一种方式,用户和域服务器之间的共享密钥泄露不会影响协议的安全性,降低了服务器密钥管理的复杂性。域间用户信息交互使用另一个域服务器的公钥加密,拥有私钥域服务器才能解密跨域信息,保证了域间信息交互的机密性。安全性分析表明本协议具有对抗包括字典攻击、重放攻击、中间人攻击等多种攻击方式的能力,并且具有前向安全性和良好的扩展性。

参 考 文 献

[1] MANNAN M, OORSCHOT P C V. A Protocol for Secure Public Instant Messaging [M]. Financial Cryptography and Data Security, 2006:20-35.

[2] CAO T, QUAN T, ZHANG B, et al. Crypt analysis of Some Client-to-Client Password-Authenticated Key Exchange Protocols[C]// 2010 3rd IEEE International Conference on Proceedings of the Broadband Network and Multimedia Technology (IC-BNMT). 2010:654-658.

[3] YAO Y, WANG X, SUN X. A Cross Heterogeneous Domain Authentication Model Based on PKI[C]// International Symposium on Proceedings of the Parallel Architectures, Algorithms and Programming. 2011:325-329.

[4] ZHANG Jiao, ZHANG Yu-jun, ZHANG Han-wen, et al. A Fast Inter-Domain Authentication Method Combining Trust Mechanism in Mobil IPv6 Networks[J]. Journal of Computer Research and Development, 2008:45(6):951-959. (in Chinese)
张娇,张玉军,张瀚文,等. 结合信任机制的移动 IPv6 网络快速跨域认证方法[J]. 计算机研究与发展,2008,45(6):951-959.

[5] BYUN J W, JEONG I R, LEE D H, et al. Password-Authenticated Key Exchange between Clients with Different Passwords [C]// Information and Communications Security, International Conference, ICICS 2002. Singapore, 2002:134-146

[6] KIM J, KIM S, KWAK J, et al. Cryptanalysis and Improvement of Password Authenticated Key Exchange Scheme between Clients with Different Passwords[C]// Computational Science and Its Applications, ICCSA 2004. Springer Berlin Heidelberg, 2004: 895-902.

[7] YOON E J, YOO K Y, et al. A secure password-authenticated key exchange between clients with different passwords[C]// Proceedings of the 2006 International Conference on Advanced Web and Network Technologies, and Applications. Springer-Verlag, 2006:659-663.

[8] LIU Xiu-mei, ZHOU Fu-cai, CHANG Gui-ran. A Verifier-Based Key Exchange Protocol in Cross-Realm Setting[C]// International Conference on Networks Security, Wireless Communications and Trusted Computing. 2009:5560-5563.

[9] FENG D G, XU J. A New Client-to-Client Password-Authenticated Key Agreement Protocol[C]// Coding and Cryptology, Second International Workshop, IWCC 2009. 2009:63-76

[10] YONEYAMA K. Cross-Realm Password-Based Server Aided Key Exchange [C]// Proceedings of the 11th International Conference on Information Security Applications. 2010:322-336.

[11] XU J, ZHU W T, JIN W T. A Generic Framework For Constructing Cross-Realm C2c-Paka Protocols Based on The Smart Card [J]. Concurrency and Computation: Practice and Experience, 2010, 23(12):1386-1398.

[12] CHUANG P J, LIAO Y P. Efficient and Secure Cross-Realm Client-to-Client Password-Authenticated Key Exchange [C]// Proceedings of the 2014 IEEE 28th International Conference on Advanced Information Networking and Applications. 2012:701-708.

[13] CHEN L, LIM H W, YANG G. Cross-domain password-based authenticated key exchange revisited[C]// Proceedings of the INFOCOM, 2013 Proceedings IEEE. 2012:1052-1060.

[14] YIN Yin, BAO L. Secure Cross-Realm C2C-PAKE Protocol [M]. Information Security and Privacy, 2006:392-406.

[15] BYUN J W, LEE D H, LIM J I. EC2C-PAKA: An efficient client-to-client password-authenticated key agreement [J]. Information Sciences: an International Journal, 2007, 177(19): 3995-3401.