标准模型下的无证书代理环签名方案

张春生[1],姚绍文[2]
(1.安庆师范学院 计算机与信息学院,安徽 安庆 246011;
2.云南大学 软件学院,云南 昆明 650091)

摘 要:由于无证书公钥密码体制是一种新型公钥密码体制,它既克服了密钥托管问题,又不需要使用公钥证书,而在标准模型下所构造的方案与在随机语言模型下所构造的方案相比,具有更高的可证安全性,因此,该文在标准模型下,提出了一个无证书代理环签名方案。与现有的代理环签名方案相比,它具有更高的执行效率和可证安全性,能够归约于CDH(computational diffie-Hellman)问题假定。分析结果表明:它既能有效抵制来自密钥生成中心和授权人的伪造攻击,又能满足代理环签名的其他安全性需求;并且,该方案具有更高的执行效率,只需要两次对运算。

关键词:无证书公钥密码体制;标准模型;环签名;代理签名;伪造攻击
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2012)11-0235-04

Certificateless Proxy Ring Signature Scheme in Standard Model

ZHANG Chun-sheng[1], YAO Shao-wen[2]
(1. College of Computer and Information, Anqing Teachers College, Anqing 246011, China;
2. College of Software, Yunnan University, Kunming 650091, China)

Abstract: Since certificateless public key cryptography (CL-PKC for short) is a new type of public key cryptography, it eliminates the key escrow problem and the need for public key certificate. And the scheme in the standard model has more provable security than the scheme in the random oracle model (ROM). So, it shows a certificateless proxy ring signature scheme in a standard model. Compared with the current proxy ring signature scheme, have the higher computing speed and more provable security, and have a security reduction to CDHP assumption. The analysis shows that it can resist forgery attacks from the secret key generation center and the original signer, and can satisfy the security requirements of a proxy ring signature scheme; meanwhile the computational efficiency is improved, the scheme only needs two bilinear parings.

Key words: certificateless public key cryptography; standard model; ring signature; proxy signature; forgery attack

0 引 言

标准模型[1,2]已经成为当前主流的密码学技术之一,在标准模型下的方案与在随机语言模型下的方案相比,具有更高的可证安全性[3]。2006年,Paterson等人在Waters签名方案的基础上提出了基于身份的签名方案[4],该方案在标准模型下被证明能够归约于CDH(computational diffie-Hellman)问题;同时,在该方案中给出了基于身份的签名方案的可证安全模型。但该方案的计算效率不高,需要多次乘法运算和多次双线性对计算。

无证书公钥密码体制[5]既解决了传统公钥密码体制中对证书的使用和验证过程,又解决了基于身份的密码系统[6]的私钥托管(key escrow)问题,其用户的签名私钥是由用户和第三方密钥生成中心KGC(key generation center)合作产生。目前,国内外学者也相继提出了一些无证书签名方案[7,8],但效率不高。

环签名由Rivest等人[9]在2001年的亚密会上提出的一种新型的签名技术,它不需要群管理员但可以实现群签名的主要功能。签名者用自己的私钥和环成员公钥进行签名,验证者可以确定签名来自一个环,但不知道真正的签名者是谁,实现了无条件匿名性。

代理签名由Mambo等人[10]1996年首次提出,原始签名者把签名权力授予一个代理者集合,每个代理者都可以代替原始签名者执行签名,验证者用原始签名者的公钥进行代理签名的验证。2003年Zhang等人[11]首次提出一种通过双线性对构建的基于身份的代理环签名方案,结合这两种签名技术实现了代理签名者的匿名性,但该方案的执行效率不高。之后相继

收稿日期:2012-03-18;**修回日期**:2012-06-25
基金项目:安徽省自然科学基金(KJ2011B077)
作者简介:张春生(1968-),男,硕士,主要研究方向为网络与信息安全;姚绍文,博士,教授,博士生导师,主要研究方向为网络协议工程、网络分布式计算。

提出的代理环签名方案存在问题[12~15]。在文献[13]中指出了文献[12]中的两个安全性错误,并给出了一个新方案。随后文献[14]指出了文献[13]也是不安全的,并进行了改进,改进的方案在代理环签名的生成时加入了原始签名人的公钥,而原始签名人的公钥是公开的,经分析也是不安全的。文献[15]将 KGC 分为多个独立的分 Trent,整个系统的安全性依赖于至少存在一个可信任的 Trent。

文中在不改变 Paterson 方案整体安全模型和困难问题假定的前提下,基于无证书公钥体制提出了一个高效安全的代理环签名方案,该方案减少了运算量,将双线性对计算次数减少到两次;同时,既能有效抵制来自 KGC 和授权人的伪造攻击,又能满足代理环签名的安全需求。

1 相关知识

1.1 双线性变换

双线性变换:设 G_1 和 G_2 分别为 q 阶的循环群,g 为 G_1 的生成元,则有 $e:G_1 \times G_1 \rightarrow G_2$,并且 e 满足条件:

(1) 双线性:对于所有的 $P,Q \in G_1$,与 $a,b \in Z_q$,都有 $e(P^a,Q^b)=e(P,Q)^{a \cdot b}$;

(2) 非退化性:$e(g,g) \neq 1$;

(3) 可计算性:存在一个有效的算法计算 $e(P,Q)$,其中 $P,Q \in G_1$。

1.2 计算 diffie-Hellman 问题

(1)离散对数问题(DLP):给定两个 $P,Q \in G_1$,找出一个整数 n,使得 $Q=nP$ 成立。

(2)定义(CDH 问题)设 G_1 为 q 阶的循环群,g 为 G_1 的生成元,对于 $\forall(g,g^a,g^b) \in G_1$,其中 $a,b \in Z_q$,计算 $g^{a \cdot b}$。

2 代理环签名的安全性要求

(1)可验证性:任何人都可以验证签名的正确性。

(2)无条件匿名性:原始签名人和任何其他第三方(包括 KGC)都不知道谁是确切的代理签名人。

(3)不可伪造性:只有授权代理人才能生成有效的代理环签名。未经授权的任何人(包括原始签名人和 KGC)都不能伪造合法的代理环签名。

(4)可区分性:代理环签名与代理人的一般环签名具有结构上的区别。

3 标准模型下的无证书代理环签名方案

3.1 方案描述

(1)系统建立(Setup):密钥生成中心(KGC)选择两个 q 阶的循环群 G_1 和 G_2,g 为 G_1 的生成元,并存在一个映射 $e:G_1 \times G_1 \rightarrow G_2$;同时,存在两个无碰撞的 Hash 函数:$H_a:\{0,1\}^* \rightarrow \{0,1\}^{n_a}$ 和 $H_b:\{0,1\}^* \rightarrow \{0,1\}^{n_b}$,两个 Hash 函数分别用于把任意长度的身份 ID 和消息 m 的二进制串映射成固定长度为 n_a 和 n_b 的二进制串。

KGC 随机选择 $x \in Z_q$,计算 $g_1=g^x$,并随机选择 $g_2 \in G_1$;同时,随机选择 $a',b' \in Z_q$ 以及两个向量 $A=(a_i)$ 和 $B=(b_i)$,其中,$a_i \in Z_q$,$b_i \in Z_q$,A 和 B 的长度分别为 n_a 和 n_b;最后,KGC 公开参数 $params=(G_1,G_2,e,g,g_1,g_2,a',A,b',B)$,系统主密钥为 g_2^x,由 KGC 秘密保管。

(2) 用户密钥生成(keyGen):

(a) 用户部分私钥生成:每个用户 $u_i(1 \leqslant i \leqslant n)$ 将其身份 ID_i 发给 KGC,KGC 计算 $Q_i=H_a(ID_i)$,Q_i 为用户身份 ID_i 的长度为 n_a 的二进制串,V_i 表示 Q_i 中比特值为 1 的位置 i 的集合,即 $V_i \subseteq \{1,2,\cdots,n_a\}$,将用户身份 ID_i 通过 V_i 映射为 $L_{ID_i}=g_2^{a'+\sum_{i \in V_i} a_i}$,则 KGC 计算用户 u_i 的部分私钥为:$d_i=g_2^x \cdot L_{ID_i}=g_2^x \cdot g_2^{a'+\sum_{i \in V_i} a_i}$,KGC 通过安全的方式发送部分私钥 d_i 给用户 u_i,用户 u_i 可以通过与 keyGen 算法同样的方式获得集合 V_i 和 L_{ID_i},然后对收到的部分私钥 d_i 进行验证:

$$e(d_i,g) \stackrel{?}{=} e(g_2,g_1) \cdot e(L_{ID_i},g)$$

如果相等,则接收;否则,可以要求 KGC 重新生成部分私钥 d_i。

(b) 用户私钥生成:每个用户 $u_i(1 \leqslant i \leqslant n)$ 随机选择一个 $x_i \in Z_q$,计算自己的签名私钥为:$d_{u_i}=g_2^{x_i} \cdot d_i=g_2^{x_i} \cdot g_2^x \cdot g_2^{a'+\sum_{i \in V_i} a_i}$,此私钥保密,由用户自己保管。

(3)代理密钥生成(proxy-keyGen):

(a)授权人 AI(原始签名者)将自己的授权信息 ω(身份、期限等),m_ω(消息集)和 $L=\{u_1,u_2,\cdots,u_n\}$(代理成员集合)发送给 KGC,KGC 首先计算 $Q_{AI}=H_a(m_\omega \| L \| \omega)$,用与 keyGen 算法同样的方式计算 $L_{AI}=g_2^{a'+\sum_{i \in V_{AI}} a_i}$,然后计算部分代理签名信息 $d'_{AI}=g_2^x \cdot L_{AI}=g_2^x \cdot g_2^{a'+\sum_{i \in V_{AI}} a_i}$,KGC 将生成嵌入 AI 信息的 d'_{AI} 通过安全的方式发送给 AI。AI 通过与 keyGen 算法同样的方式获得集合 V_i 和 L_{AI},然后对收到的 d'_{AI} 进行验证:

$$e(d'_{AI},g) \stackrel{?}{=} e(g_2,g_1) \cdot e(L_{AI},g)$$

如果相等,则接收;否则,可以要求 KGC 重新生成部分代理签名信息 d'_{AI}。

(b) AI 在确认部分代理签名信息 d'_{AI} 合法后,随机选择个 $x_{AI} \in Z_q$,计算授权代理签名信息:(t,d_{AI}),

其中 $t=g^{x_w}$，$d_{AI}=g_2^{x_w}\cdot d'_{AI}=g_2^{x_w}\cdot g_2^{x}\cdot g_2^{a'+\sum a_i}$，然后将 (t,d_{AI}) 对发送给授权的代理签名成员 $u_i\in L(1\leqslant i\leqslant n)$。

(c)假设环中的真正代理签名成员 $u_s\in L$（其私钥为 $d_{u_s}=g_2^{x_s}\cdot g_2^{x}\cdot g_2^{a'+\sum a_i}$），在接收到 AI 发来的代理签名信息 (t,d_{AI}) 后，首先用与 keyGen 算法同样的方式计算出 $L_{AI}=g_2^{a'+\sum a_i}$，然后验证：

$$e(d_{AI},g)\overset{?}{=}e(g_2,g_1)\cdot e(L_{AI},g)\cdot e(g_2,t)$$

如果相等，则是来自于 AI 的授权签名信息；否则，拒绝接收。

u_s 验证后，计算自己的代理签名密钥：

$$d_{SAI}=d_{u_s}\cdot d_{AI}$$

(4) 代理环签名算法(Sign)：当 u_s 代表 L 签署 m_ω 所允许的消息 m 时，计算过程如下：

u_s 随机选取 $R_i\in Z_q$ $(i=1,\cdots,n,i\neq s)$，计算：

$$M_i=H_b(m\,||\,L\,||\,R_i)\tag{1}$$

通过与 keyGen 同样的方法对长度为 n_b 的 M_i 的二进制串进行处理，获得 W_i 的集合，W_i 表示 M_i 中比特值为 1 的位置 j 的集合，即 $W_i\subseteq\{1,2,\cdots,n_b\}$，则消息 m 映射为：

$$N_i=g_2^{b'+\sum b_j}\tag{2}$$

u_s 随机选择 $r\in Z_q$，进行如下计算：$\beta=g^r$

$$R_s=g_2^{r}\cdot d_{SAI}-\sum_{i=1,i\neq s}^{n}(R_i+N_i\cdot L_{ID_i})\tag{3}$$

$M_s=H_b(m\,||\,L\,||\,R_s)$，通过与(2)式同样的方法计算 $N_s=g_2^{b'+\sum b_j}$，然后计算

$$C=(g_2^{r}\cdot d_{SAI}+N_s\cdot L_{ID_s})^{r}\tag{4}$$

则对消息 m 的代理环签名为：

$$\sigma=(m,L,R_1,\cdots,R_n,C,\beta)$$

(5)验证算法(Verify)：签名接收者收到代理环签名 $\sigma=(m,L,R_1,\cdots,R_n,C,\beta)$ 后，可以通过以下计算进行验证：

对所有的 $i\in[1,n]$，先计算 $M_i=H_b(m\,||\,L\,||\,R_i)$，用与签名者同样的方法计算 $N_i=g_2^{b'+\sum b_j}$，用与 KGC 同样的方法计算 $L_{ID_i}=g_2^{a'+\sum a_i}$，当且仅当等式：

$$e\Big(\sum_{i=1}^{n}(R_i+N_i\cdot L_{ID_i}),\beta\Big)=e(C,g)\tag{5}$$

成立，则签名 $\sigma=(m,L,R_1,\cdots,R_n,C,\beta)$ 有效，否则签名无效。

3.2　方案分析

3.2.1　正确性分析

(1) 任一用户 u_i 对自己的部分私钥 d_i 进行验证。

定理 1 如果 $d_i=g_2^{x}\cdot L_{ID_i}=g_2^{x}\cdot g_2^{a'+\sum a_i}$ 是成员 u_i 有效的部分私钥，则等式 $e(d_i,g)=e(g_2,g_1)\cdot e(L_{ID_i},g)$ 必定成立。

证明：

$$e(d_i,g)=e(g_2^{x}\cdot g_2^{a'+\sum a_i},g)=e(g_2^{x},g)\cdot e(g_2^{a'+\sum a_i},g)=e(g_2,g_1)\cdot e(L_{ID_i},g)$$

同理可以证明授权人 AI 的部分代理签名信息 d'_{AI} 的验证式 $e(d'_{AI},g)=e(g_2,g_1)\cdot e(L_{AI},g)$。

(2) 代理签名人 u_s 对授权人 AI 发来的代理签名信息 (t,d_{AI}) 进行验证：

定理 2 如果代理签名信息 (t,d_{AI}) 确是来自于 AI 的授权签名信息，则下面的等式必定成立

$$e(d_{AI},g)=e(g_2,g_1)\cdot e(L_{AI},g)\cdot e(g_2,t)$$

证明：由 $d_{AI}=g_2^{x_w}\cdot g_2^{x}\cdot g_2^{a'+\sum a_i}$，$t=g^{x_w}$ 得：

$$\begin{aligned}e(d_{AI},g)&=e(g_2^{x_w}\cdot g_2^{x}\cdot g_2^{a'+\sum a_i},g)\\&=e(g_2^{x},g)\cdot e(g_2^{a'+\sum a_i},g)\cdot e(g_2^{x_w},g)\\&=e(g_2,g_1)\cdot e(L_{AI},g)\cdot e(g_2,t)\end{aligned}$$

(3) 签名接收者对签名者 u_s 对消息 m 的代理环签名 $\sigma=(m,L,R_1,\cdots,R_n,C,\beta)$ 进行验证。

定理 3 如果代理签名者 u_s 对消息 m 的代理环签名 $\sigma=(m,L,R_1,\cdots,R_n,C,\beta)$ 是有效的，则等式 $e\Big(\sum_{i=1}^{n}(R_i+N_i\cdot L_{ID_i}),\beta\Big)=e(C,g)$ 必定成立。

证明：由(3)、(4)式，有

$$\begin{aligned}&e\Big(\sum_{i=1}^{n}(R_i+N_i\cdot L_{ID_i}),\beta\Big)\\&=e\Big(R_s+N_s\cdot L_{ID_s}+\sum_{i=1,i\neq s}^{n}(R_i+N_i\cdot L_{ID_i}),g^r\Big)\\&=e\Big(g_2^{r}\cdot d_{SAI}-\sum_{i=1,i\neq s}^{n}(R_i+N_i\cdot L_{ID_i})+N_s\cdot L_{ID_s}+\\&\quad\sum_{i=1,i\neq s}^{n}(R_i+N_i\cdot L_{ID_i}),g^r\Big)\\&=e(g_2^{r}\cdot d_{SAI}+N_s\cdot L_{ID_s},g^r)\\&=e((g_2^{r}\cdot d_{SAI}+N_s\cdot L_{ID_s})^{r},g)\\&=e(C,g)\end{aligned}$$

3.2.2　安全性分析

(1)可验证性：由定理 3 可知，任何人都可以验证签名的正确性。

(2)无条件匿名性(无条件匿名性参照文献[15]中证明方法)：

因为所有的 $R_i\in Z_q$ 都是在域上均匀随机选择的，并不包含任何签名者的信息，故依次选出 $R_1,\cdots,R_n\in Z_q$ $(i=1,\cdots,n,i\neq s)$ 的概率为：

$$\frac{1}{q-1}\times\frac{1}{q-2}\times\cdots\times\frac{1}{q-n+1}$$

对签名者来说，虽然在生成签名时所使用的代理签名密钥中包含自己的私钥，嵌入了签名者的信息，但是通过(3)式计算被 r 随机化后不再包含签名者的

任何信息。故依次选出所有的 $R_1,\cdots,R_n$ $(i=1,\cdots,n)$ 的概率为：

$$\frac{1}{q-1}\times\frac{1}{q-2}\times\cdots\times\frac{1}{q-n}$$

由此可见能确定真正签名者的概率不超过 $1/n$（n 为环成员的个数），所以该方案满足签名者的无条件匿名性。

(3)定理 4 给出的方案满足不可伪造性。任何人（包括原始签名人和 KGC）不能伪造一个不包括自己的环签名。

证明：

假设敌手 $u_i \notin L=\{u_1,u_2,\cdots,u_n\}$（包括授权人和 KGC），他能够成功伪造一个有效的代理环签名 $\sigma=(m,L,R_1,\cdots,R_n,N_1,\cdots,N_n,C,\beta)$，根据环签名的分叉引理[16]可知，存在一个算法，能以不可忽略的概率输出 2 个有效的代理环签名

$\sigma=(m,L,R_1,\cdots,R_n,N_1,\cdots,N_n,C,\beta)$ 和

$\sigma'=(m,L,R_1,\cdots,R_n,N_1',\cdots,N_n',C',\beta)$，

其中 $N_i=N_i'(i\neq s)$，而 $N_s\neq N_s'$，由于 2 个签名均有效，故满足签名验证方程，于是有：

$$e\Big(\sum_{i=1}^{n}(R_i+N_i\cdot L_{ID_i}),\beta\Big)=e(C,g)$$

$$e\Big(\sum_{i=1}^{n}(R_i+N_i'\cdot L_{ID_i}),\beta\Big)=e(C',g)$$

由以上两个等式得：

$e(N_s\cdot L_{ID_s}-N_s'\cdot L_{ID_s}',\beta)=e((C-C'),g)$，则有

$$e((N_s\cdot L_{ID_s}-N_s'\cdot L_{ID_s}')^{r},g)=e((C-C'),g)$$

即 $(N_s\cdot L_{ID_s}-N_s'\cdot L_{ID_s}')^{r}=C-C'$，因此解决了一个 CDHP 难题。

(4)可区分性：由公式 $d_{SAI}=d_{u_s}\cdot d_{AI}$ 可知，代理签名钥 d_{SAI} 是在代理签名者的私钥 d_{u_s} 中嵌入了授权人的信息 d_{AI}，所以生成的代理环签名与一般环签名具有结构上的区别，因此该签名方案具有很好的可区分性。

3.2.3 效率分析

由于系统建立、用户密钥生成和代理签名密钥生成都可以在签名之前完成，而且时间开销不大，所以本方案的效率分析主要考虑代理环签名和签名的验证两个阶段。如果用 C_{add} 表示加运算，用 $C_{1\ mul}$ 和 $C_{2\ mul}$ 分别表示 G_1 和 G_2 中的乘运算，$C_{pairing}$ 表示对 e 的运算。则与文献[11,13]的比较见表 1 。

双线性对的运算时间是影响签名方案效率的关键性因素。从表 1 可看出，提出的方案只在验证签名时进行 2 次对运算，文献[11]需要进行 $4n-1$ 次对运算，文献[13]虽然进行 2 次对运算，但该方案是不安全的。本方案同时又能有效地克服密钥托管问题。

表 1 文中方案与文献[11,13]的比较

	Zhang[11]	罗[13]	文中方案
C_{add}	$2n$	$4n$	$4n$
$C_{1\ mul}$	$2n$	$4n$	$2n$
$C_{2\ mul}$	$n-1$	0	$2n$
$C_{pairing}$	$4n-1$	2	2
能否避免密钥托管问题	不能	不能	能

4 结束语

文中给出了标准模型下的无证书代理环签名方案的构造过程，并给出了方案的正确性证明、安全性分析和效率分析。方案能有效抵制来自 KGC 和授权人的伪造攻击和可能的联合攻击，并满足代理环签名所要求的多种安全性质。无证书密码体制解决了密钥托管和证书管理问题。本签名方案可以广泛应用于电子投标、电子支付等领域。

参考文献：

[1] Boneh D, Boyen X. Secure identity-based encryption without random oracles[C]//Proc. of the Advances in Cryptology-CRYPTO. Berlin: Springer-Verlag, 2004: 443-459.

[2] Waters B. Efficient identity-based encryption without random oracles[C]//Advances in Cryptology-EUROCRYPT 2005. Berlin: Springer-Verlag, 2005: 114-127.

[3] 谷 科，贾维嘉，姜春林. 高效安全的基于身份的签名方案[J]. 软件学报，2011，22(6)：1350-1360.

[4] Paterson K G, Schuldt J C N. Efficient identity-based signatures secure in the standard model[C]//Proc. of the ACISP 2006. Berlin: Springer-Verlag, 2006: 207-222.

[5] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[C]//Proc. of the ASIACRYPT 2003. Berlin: Springer-Verlag, 2003: 452-473.

[6] Shamir A. Identity-based cryptosystems and signature schemes[C]//Proceedings of Crypto 1984. Berlin: Springer Verlag, 1985: 47-53.

[7] Hu B, Wong D, Zhang F, et al. Key replacement attack against a generic construction of certificateless signature[C]//Advances in ACISP 2006, Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2006: 235-246.

[8] Yap W, Heng S, Goi B. An efficient certificateless signature scheme[C]//Proc. of EUC Workshop 2006, Lecture Notes in Computer Science. Berlin: [s. n.], 2006: 322-331.

[9] Rivest R L, Shamir A, Tauman Y. How to Leak a Secret 17th International Conference on the Theory and Application of Cryptology and Information Security[C]//LNCS 2248. Berlin: Springer-Verlag, 2001: 552-565.

[10] Mambo M, Usuda K, Okamoto E. Proxy Signatures: Delegation

（下转第 242 页）

止窃取者非法获取图像信息，加密后的图像相邻的像素之间应该具有比较低的相关系数，通过下面的公式来分别计算它们垂直、水平、对角的关联系数[11]。

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{5}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x)]^2 \tag{6}$$

$$\mathrm{COV}(x,y)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x)][y_i-E(y)] \tag{7}$$

$$R(x,y)=\frac{\mathrm{COV}(x,y)}{\sqrt{D(x)D(y)}} \tag{8}$$

其中，x 和 y 表示图像中两相邻像素的灰度值，从原始和加密后的图像中，随机选择其中任意 512 对两个相邻的像素点，根据以上公式计算出它们各自的相关系数，并与采用像素置乱方法加密后的图像和采用文献[12]方法加密后的图像的相关性进行比较。

从表 1 可以看出，原始图像的两相邻像素的相关系数近似等于 1，是强相关；而采用本算法的加密后的图像中的两个相邻像素之间的相关系数几乎为 0，可见它们的相关性很低。与仅对图像像素进行置乱的方法加密后的和文献[6]加密方法后的实验结果相比较，可以得出本算法的实验效果更好。

表 1 相邻像素的相关系数

方向	原始图像	加密后的图像	采用像素置乱方法加密后的图像	采用文献[12]方法加密后的图像
水平	0.9846	0.0258	0.03058	0.01578
垂直	0.9711	0.0368	0.06362	0.06533
对角	0.9555	0.0410	0.02718	0.03222

4 结束语

文中提出了一种基于交叉混沌的加密算法，经过分析，由 Logistic 映射和 Chebyshev 映射组成的多混沌图像加密算法，输出的图像像素具有良好的自相关性和互相关性，混沌系统的加密模型复杂，克服了加密的初始密钥空间不足的弱点，既保证了图像加密的安全性，抵抗非法用户使用多种攻击手段，又提高了对图像处理的效率。只有利用正确的算法和密钥，才可以对加密图像进行正确解密。

从实验的结果可以看出，该加密算法具有很好的安全性，在信息安全领域有较好的应用前景和研究价值。

参考文献：

[1] Yassen M T. Chaos Control of Chen Chaotic Dynamical System [J]. Chaos, Solitons & Fractals, 2003, 15(2): 271-283.

[2] 孙世良. 基于混沌理论的密码技术[D]. 哈尔滨：哈尔滨工程大学，2006.

[3] Ueta T, Chen G R. Bifurcation Analysis of Chen's Equation [J]. International Journal of Bifurcation and Chaos, 2000, 10(8): 1917-1931.

[4] 冯 勇. 二维混沌映射图像加密安全性分析及改进算法[J]. 哈尔滨工业大学学报，2007，39(9)：1411-1414.

[5] 王 永. 混沌加密算法与 Hash 函数构造研究[M]. 北京：电子工业出版社，2011.

[6] 王银花，王丽萍. 基于分频域相位和幅度的数字图像加密新方法[J]. 计算机技术与发展，2009，19(4)：177-183.

[7] Zhang Yonghong, Kang Baosheng, Zhang Xuefeng. Image Encryption Algorithm Based on Chaotic Sequence [C]//The 16th International Conference on Artificial Reality and Telexistence. [s. l.]: [s. n.], 2006.

[8] 叶瑞松，兀松贤. 一个对称的四维混沌系统及其图像隐藏应用[J]. 计算机技术与发展，2010，20(1)：93-96.

[9] 郭现峰. 基于混沌动态 S 盒的密码算法及其应用研究[D]. 成都：西南交通大学，2011.

[10] 李传目，洪联系，万 春. 基于混沌序列的图像分块加密方法[J]. 计算机技术与发展，2007，17(8)：51-54.

[11] 尹 萍，闵乐泉. 基于离散广义同步定理的复合混沌音频加密方案[J]. 计算机科学，2011，38(4)：104-106.

[12] Lian Shiguo, Sun Jinsheng, Wang Jinwei. A chaotic stream cipher and the usage in video protection[J]. Chaos, Solitons and Fractals, 2007, 34(3): 851-859.

（上接第 238 页）

of the Power to Sign Messages[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1996, 79(9): 1338-1354.

[11] Zhang F, Naini R, Lin C Y. New proxy signature, proxy blind signature and proxy ring signature schemes from bilinear pairings[EB/OL]. [2003-05-20]. Cryptolgy ePrint Archive. http://eprint.iacr.org/2003/.

[12] 禹 勇，杨 波，李发根，等. 一个有效的代理环签名方案[J]. 北京邮电大学学报，2007，30(3)：23-26.

[13] 罗大文，何明星，李 娥. 一种新的可证明安全的代理环签名方案[J]. 计算机工程与应用，2009，45(7)：100-102.

[14] 张小萍，钟 诚. 改进的代理环签名方案[J]. 计算机应用研究，2011，28(9)：3505-3507.

[15] 陈 珂，苗付友，熊 焰. 基于 RSA 的代理环签名方案[J]. 计算机科学，2009，36(2)：132-136.

[16] Herranz J, Saez G. Forking Lemmas for Ring Signature Schemes[C]//INDOCRYPT 2003. Berlin: Springer-Verlag, 2003: 266-279.