基于XTR机制改进的直接匿名认证方案

杨亚涛[1] 曹陆林[1] 李子臣[1] 郭宝安[2] 徐树民[2]
(北京电子科技学院 北京 100070)[1] (航天信息股份有限公司 北京 100195)[2]

摘 要 现有的直接匿名认证方案吸取了群签名、身份托管、证书系统等技术来实现匿名证明,存在着执行效率慢、安全性差等缺点;而新型XTR公钥密码体制运算速度快,安全性强。基于XTR公钥密码体制,采用零知识证明的思路,改进了目前的直接匿名认证方案,经分析论证,与原机制相比,新方案的安全性和执行效率均得到明显提高。

关键词 可信计算,直接匿名认证,XTR
中图法分类号 TP393.08 **文献标识码** A

Improved Direct Anonymous Attestation Scheme Based on XTR System

YANG Ya-tao[1] CAO Lu-lin[1] LI Zi-chen[1] GUO Bao-an[2] XU Shu-min[2]
(Beijing Electronic Science and Technology Institute, Beijing 100070, China)[1]
(AISINO CO. LTD., Beijing 100195, China)[2]

Abstract The existing direct anonymous attestation scheme achieves anonymous attestation using group signature, identity managed, certificate system technology and so on, which has the defect being slow implementation of the efficiency and poor safety. The computing speed of the new XTR public key cryptosystem is fast, and its safety is well. Based on the XTR public key cryptosystem, using zero-knowledge proof, this article improved the original direct anonymous attestation scheme. Demonstrated by analyzing, compared with the original mechanism, the security and implementation of this new scheme have been improved greatly.

Keywords Trusted computing, Direct anonymous attestation, XTR

1 引言

伴随着数字时代的到来,网络以及电子商务的发展已经给人们的生活带来了巨大的便利,随之而来的信息安全问题也日益突出。目前,可信计算技术成为了信息安全领域研究的热点,而远程认证又是可信计算研究的关键技术。远程认证是请求者向远程验证者证明自己的身份以及平台配置的过程。可信计算组织(TCG)认为保护用户隐私是远程认证必须考虑的问题,远程平台在执行认证的同时也要保护自己平台的隐私信息,以及防止平台行为被跟踪。TCG在规范TPMv1.1中发布了Privacy CA方案,规定TPM(Trusted Platform Module)的合法性由Privacy CA负责验证,但是每次认证时Privacy CA都必须参与到其中,进而会成为影响认证效率的瓶颈。为解决这一问题,2003年10月TCG发布了TPMv1.2,提出了一种直接匿名认证(Direct Anonymous Attestation,DAA)方案[1,2],较好地解决了Privacy CA方案中的缺陷问题,但却以执行庞大的计算作为代价[3]。针对这一不足,在TCG规范的基础上,提出了诸多对原直接匿名证明方案的改进。文献[5]在决策Diffie-Hellman和q-SDH[4]假设的基础上,对原方案进行了改进,缩短了私钥和签名长度,同时提高了安全性。文献[6]在椭圆曲线和双线性映射的基础上,首次详细地提出了BCL-DAA方案,有效地降低了可信平台模块TPM的运算成本,并提高了方案的安全性。文献[7]对文献[6]中的DAA协议做了进一步的优化,使得TPM、主机、验证者的计算效率同时得到了提高,并在随机预言模型l-MOMSDH假设下证明是安全的。但是,以上方案都是建立在RSA或ECC(Elliptic Curve Cryptography)公钥密码体制的基础上,而新型的XTR公钥密码体制能够保证安全性和ECC公钥密码体制基本一致的情况下,其求幂运算比ECC公钥密码体制中的倍点运算要快,更远大于RSA公钥密码体制中的求幂运算。而且在密钥选取的速度上,XTR公钥密码体制与RSA公钥密码体制相当,比ECC公钥密码体制要快几个数量级。同时,由于XTR公钥密码体制采用的数学函数比ECC公钥密码体制更直接,使得应用更加方便。基于此,本文在XTR公钥密码体制的基础上,设计了一种新的直接匿名证明方案。经论证分析,新方案的执行效率和安全性都得到了进一步的提高。

2 基本知识

XTR(Efficient and Compact Subgroup Trace Representa-

到稿日期:2010-05-01 返修日期:2010-09-01 本文受北京电子科技学院信息安全重点实验室资助课题,国家自然科学基金项目(61070219),国家商用密码应用技术体系研究及应用示范项目电子标签应用示范工程课题(2008BAH22B04)资助。
杨亚涛(1978-),男,博士,讲师,主要研究方向为网络安全、可信计算等,E-mail:yy2008@163.com;曹陆林(1985-),男,硕士生,主要研究方向为可信计算等;李子臣(1965-),男,博士,教授,主要研究方向为密码学、可信计算等;郭宝安(1963-),男,博士,主要研究方向为信息安全;徐树民 男,研究员,高工,主要研究方向为信息安全与芯片设计。

tion)是有效紧致子群的迹表示的缩写，是由 Lenstra 和 Verheul 在 Crypto 2000 提出的一种新型公钥密码体制。自从 2000 年 Lenstra 在美密会上提出了 XTR 公钥密码体制后，由于该体制运算速度快，资源占用量少，一直受到人们的广泛关注。

定义 1 已知 $c=Tr(g)\in GF(p^2)$，$c_k=Tr(g^k)\in GF(p^2)$，$1\leqslant k\leqslant q$，k 的值在计算上是不可行的。这称为求解迹离散对数问题(XTR-DL)。

XTR 公钥密码体制的安全性是基于在 XTR 群中求解离散对数问题的困难性。在 XTR 体制下求解 XTR-DL 问题的困难程度相当于在 $GF(p^6)^*$ 中求解离散对数问题的难度。在文献[8]中给出求迹函数的快速算法，已知 $Tr(g)$ 和 k 时，求解 $Tr(g^k)$ 的计算量相当于在 $GF(p)$ 中进行 $8\log_2 k$ 次乘法运算，比已知 g 和 k 时计算 g^k 的运算速度快大约 3 倍。并且因为 $g^k\in GF(p^6)^*$，而 $Tr(g^k)\in GF(p^2)$，所以 $Tr(g^k)$ 的表示、存储、传输所需要的时间和空间复杂度都是 g^k 的 1/3。

在相同应用体制和安全性的条件下，XTR 公钥密码体制的运算速度大约是 ElGamal、RSA 公钥密码体制的 3 倍，而密钥长度、信息存储量和通信传输量大约只有它们的三分之一。与 ECC 公钥密码体制相比，XTR 公钥密码体制的密钥生成速度比 ECC 公钥密码体制快几个数量级，而且不会选到影响安全性的参数，无需对新得到的结果附加测试。

3 改进的基于 XTR 的 DAA 方案

定义 2 元素 $\dot{N}$ 的迹为 N。即 $N=Tr(\dot{N})$。

3.1 DAA 发布者设置

1)发布者选择素数 $p\equiv 2 \bmod 3$，$q>3$ 且 $q\mid p^2-p+1$，g' 的阶为 q。

2)产生随机整数 $x_0,x_1,x_z,x_s,x_h,x_g,x_k,k,r$，我们用以下参数表示。

$\dot{g}:=g'^{x_g}\quad \dot{h}:=g'^{x_h}\quad \dot{S}:=h^{x_s}\quad \dot{Z}:=h^{x_z}$

$\dot{R}_0:=S^{x_0}\quad \dot{R}_1:=S^{x_1}\quad \dot{m}=h^k\quad \dot{n}=h^r$

相关迹函数为 g,h,S,Z,R_0,R_1,m,n。

3)选择随机数 ρ 和 Γ，让 $\Gamma=\gamma\rho+1$ 同时保证 ρ 不能整除 γ，$2^{l_\Gamma-1}<\Gamma<2^{l_\Gamma}$，$2^{l_\rho-1}<\rho<2^{l_\rho}$ 选择 $\gamma'\in_R Z_\Gamma^*$，$\gamma'^{(\Gamma-1)/\rho}\neq 1 \pmod\Gamma$，$\gamma:=\gamma'^{(\Gamma-1)/\rho} \bmod \Gamma$

4)公布公钥

$(Tr(g'),g,h,S,Z,R_0,R_1,m,n,k,\gamma,\Gamma,\rho)$ 并把 g',k,r 作为私钥密存。

3.2 加入协议

1)host 计算 $\zeta_I:=(H_\Gamma(1||bsn_I))^{(\Gamma-1)/\rho} \bmod \Gamma$ 并把 ζ_I 传递给 TPM。

2)TPM 验证 $\zeta_I^\rho\equiv 1 \pmod\Gamma$ 产生 (f_0,f_1)，$v'\in_R\{0,1\}^{l_q+l_\phi}$。计算 $U:=Tr(\dot{S}^{x_0 f_0}\dot{S}^{x_1 f_1}\dot{S}^{v'})$，$N_I:=\zeta_I^{f_0+f_1 2^{l_f}} \bmod \Gamma$ 并将 U 和 N_I 发送给 host。

3)DAA 发布者检验泄露列表中所有的 (f_0,f_1) 是否有 $N_I\overset{?}{\neq}(\zeta_I^{f_0+f_1 2^{l_f}}) \pmod\Gamma$。

如果 DAA 发布者发现 N_I 以前使用过，就认为 TPM 不合法，则终止协议。验证为 TPM 合法，则进行证明协议。

4)TPM 向 DAA 发布者进行关于 f_0,f_1 和 v' 的零知识证明。协议如下：

(a)TPM 选择随机整数 $r_{f_0},r_{f_1}\in_R\{0,1\}^{l_f+l_\phi+l_H}$，$r_{v'}\in_R\{0,1\}^{l_q+2l_\phi+l_H}$，计算 $\tilde{U}:=Tr(\dot{S}^{x_0 r_{f_0}+x_1 r_{f_1}+x_s r_{v'}})$，$\tilde{N}_I:=\zeta^{r_{f_0}}+r_{f_1}^{2^{l_f}} \bmod \Gamma$ 并将 $\tilde{U}$ 和 $\tilde{N}_I$ 发送给 host。

(b) DAA 发布者选择随机整数 $n_i\in\{0,1\}^{l_H}$，并将 n_i 发送给 host。

(c) host 计算 $c_h=H(q||R_0||R_1||S||U||N_I||\tilde{U}||\tilde{N}_I||_{ni})$ 并发给 TPM。

(d) TPM 随机选择 $n_t\in_R\{0,1\}^{l_\phi}$，计算 $c:=H(c_h||n_t)\in[0,2^{l_H-1}]$

(e) TPM 计算 $s_{f_0}:=r_{f_0}+cf_0$，$s_{f_1}:=r_{f_1}+cf_1$，$s_{v'}:=r_{v'}+cv'$ 并把 $(c,n_t,s_{f_0},s_{f_1},s_{v'})$ 发送给 host。

(f) host 把 $(c,n_t,s_{f_0},s_{f_1},s_{v'})$ 发送给 DAA 发布者。

(g) DAA 发布者计算 $(c,n_t,s_{f_0},s_{f_1},s_{v'})$，$U_S:=Tr(\dot{S}^{x_0 s_{f_0}+x_1 s_{f_1}+s_{v'}})$，$U^{-c}:=Tr(\dot{S}^{-c(x_0 f_0+x_1 f_1+v')})$，$\hat{U}:=Tr(\dot{U}^{-c}U_S)$

然后检查

$$c_h\overset{?}{=}H(H(q||R_0||R_1||S||U||N_I||\hat{U}||\hat{N}_I||n_i)n_t)$$

5)DAA 发布者选择 $\hat{v}\in_R\{0,1\}^{l_v-1}$ 和素数 $e\in_R[2^{l_e-1},2^{l_e-1}+2^{l'_e-1}]$，计算 $v''=\hat{v}+2^{l_v-1}$，$s=ke+r \pmod q$，$A:=Tr((\dot{Z}\dot{U}^{-1}\dot{S}^{-v''})^{1/e}\dot{h}^k)$。

6)DAA 发布者与 host 之间进行关于 A 的零知识证明协议。

(a) host 选择随机整数 $n_h\in_R\{0,1\}$ 并将 n_h 发送给 DAA 发布者。

(b) DAA 发布者随机选择 $r_e\in[0,q]$ 并计算

$\tilde{A}:=Tr((\dot{Z}\dot{U}^{-1}\dot{S}^{-v''})^{r_e})$

$c':=H(q||Z||S||U||v''||A||\tilde{A}||n_h)$

$s_e:=r_e-c'/e$

将 c',s_e 和 (A,e,s,v'') 发给 host。

(c) host 计算

$A^{c'}:=Tr((\dot{Z}\dot{U}^{-1}\dot{S}^{-v''})^{c'/e})$

$A^{s_e}:=Tr((\dot{Z}\dot{U}^{-1}\dot{S}^{-v''})^{s_e})$

$\hat{A}:=Tr(\dot{A}^{c'}\dot{A}^{s_e})$

验证

$c'\overset{?}{=}H(q||Z||S||U||v''||A||\hat{A}||n_h)$ 和 $Tr(h^s)\overset{?}{=}Tr(h^{ek}h^r)$。

7)host 将 v'' 发送给 TPM。

8)TPM 收到 v'' 后，计算 $v:=v''+v'$ 然后将 (f_0,f_1,v) 储存。

3.3 签名协议

1)依据验证者的要求，host 如下计算 $\zeta\in_R(\gamma)$ 或者 $\zeta:=(H_\Gamma(1||bsn_i))^{(\Gamma-1)/\rho} \bmod \Gamma$，然后将 ζ 发送给 TPM。然后，TPM 检测是否 $\zeta^\rho\equiv 1 \pmod\Gamma$。

2)host 选择随机数 $w,r\in_R\{0,1\}^{l_q+l_\Phi}$ 并计算 $T_1:=Tr(\dot{A}^e\dot{h}^w)$，$T_2:=Tr(\dot{g}^w\dot{h}^e(g')^r)$

然后，TPM 计算 $N_v:=\zeta^{f_0+f_1 2^{l_f}} \bmod \Gamma$ 将 N_v 发送给 host。

3)host 和 TPM 一起完成签名。

(a) 首先，TPM 选择随机数 $w,r_v\in_R\{0,1\}^{l_v+l_\Phi+l_H}$ 和 $r_{f_0},r_{f_1}\in_R\{0,1\}^{l_f+l_\Phi+l_H}$ 并计算 $\tilde{T}_{1t}:=Tr(\dot{R}_0^{r_{f_0}}\dot{R}_{f_1}^{r_{f_1}}\dot{S}^{r_v})=Tr(\dot{S}^{x_0 r_{f_0}+x_1 r_{f_1}+r_v})$，$\tilde{r}_f:=r_{f_0}+r_{f_1}2^{l_f} \bmod \rho$，$\tilde{N}_v:=\zeta^{r_f} \bmod \Gamma$

然后，host 选择随机数

$r_e,r_s\in_R\{0,1\}^{l'_e+l_\phi+l_H}$

$r_{ee} \in_R \{0,1\}^{2l_e+l_\phi+l_H+1}$

$r_w, r_r \in_R \{0,1\}^{l_q+2l_\phi+l_H}$

$r_{ew}, r_{er} \in_R \{0,1\}^{l_e+l_q+2l_\phi+l_H+1}$

再计算：

$\tilde{T}_1 := Tr(\dot{\tilde{T}}_{1t}\tilde{T}_1^{r_e}\dot{h}^{-r_{ew}}\dot{h}^{r_s})$

$\tilde{T}_2 := Tr(\dot{g}^{r_w}\dot{h}^{r_e}\dot{g}'^{r_r})$

$c_h := H((q)||Tr(g')||g||h||R_0||R_1||S||Z||\gamma||\Gamma||\rho)||\zeta||T_1||T_2||N_v||(\tilde{T}_1||\tilde{T}_2||\tilde{T}'_2)||\tilde{N}_v)$

$\tilde{T}'_2 := Tr(\tilde{T}_2^{-r_e}\dot{g}^{r_{ew}}\dot{h}^{r_{ee}}\dot{g}'^{r_{er}})$ 。

(b) host 将 c_h 发送给 TPM。

TPM 选择随机数 $n_t \in \{0,1\}^{l_\varphi}$，计算 $c := H(c_h||n_t||m)$，然后将 c 发送给 host。

(c) TPM 计算 $s_v := r_v + cv, s_{f_0} := r_{f_0} + cf_0, s_{f_1} := r_{f_1} + cf_1$，然后将 (s_v, s_{f_0}, s_{f_1}) 发送给 host。

host 还要计算

$s_e := r_e + c \cdot (e - 2^{l_e-1})$

$s_{ee} := r_{ee} + ce^2$

$s_w := r_w + c \cdot w$

$s_{ew} := r_{ew} + c \cdot w \cdot e$

$s_r := r_r + c \cdot r$

$s_{er} := r_{er} + c \cdot e \cdot r$

$s_s := r_s - cs$

4)host 输出签名

$\sigma := (\zeta, (T_1, T_2), N_v, c, n_t, (s_v, s_{f_0}, s_{f_1}, s_e, s_{ee}, s_w, s_{ew}, s_r, s_{er}, s_s))$

3.4 验证协议

关于信息 m 的签名验证者的验证如下。

1)计算

$\hat{T}_1 := Tr(\dot{h}^{-cz}\dot{T}_1^{s_e+c2^{l_e-1}}\dot{h}^{cr}\dot{h}^{s_s}R_0^{s_{f_0}}R_1^{s_{f_1}}S^{s_v}\dot{h}^{-s_{ew}})$

$\hat{T}_2 := Tr(\dot{T}_2^{-c}\dot{g}^{s_w}\dot{h}^{s_e+c2^{l_e-1}}\dot{g}'^{s_r})$

$\hat{T}_2' := Tr(\dot{T}_2^{-(s_e+c2^{l_e-1})}\dot{g}^{s_{ew}}\dot{h}^{s_{ee}}\dot{g}'^{s_{er}})$

$\hat{N}_v := N_v^{-c}\zeta^{s_{f_0}+s_{f_1}2^{l_f}} \bmod \Gamma$

2)验证

$c \stackrel{?}{=} H(H((q)||Tr(g')||g||h||R_0||R_1||S||Z||\gamma||\Gamma||\rho)||\zeta||T_1||T_2||N_v||(\hat{T}_1||\hat{T}_2||\hat{T}'_2)||\tilde{N}_v)||n_t||m)$

$N_v, \zeta \stackrel{?}{\in} [\gamma], s_{f_0}, s_{f_1} \stackrel{?}{\in}_R \{0,1\}^{l_f+l_\phi+1}, s_e \stackrel{?}{\in}_R \{0,1\}^{l'_e+l_\phi+l_H+1}$

3)检验所有的 (f_0, f_1) 列表 $N_v \stackrel{?}{\equiv} \zeta^{f_0+f_1 2^{l_f}} \pmod{\Gamma}$。

4 性能分析

4.1 安全性分析

本文提出的 DAA 改进方案是基于 XTR 公钥密码体制的，所以具有 XTR 体制的安全性。XTR 体制算法是基于求解有限域上元素的迹函数离散对数困难问题。已知 $c_k = Tr(g^k)$，$1<k<q$，求 k 的值在计算上是不可行的。这称为求解离散对数问题(XTR-DL)。在 XTR 体制下求解 XTR-DL 问题的困难程度与在 $GF(p^6)^*$ 中求解离散对数问题的难度相同。

改进方案的安全性基于 XTR 离散对数问题。当 p, q 取 170 位的素数，则改进的 DAA 方案比基于 1024 位的 RSA 公钥密码体制的 DAA 方案更为安全。

在改进的 DAA 方案中用户想伪造出一个符合要求的 (A, e, s)，只能从 $Tr(h^k), Tr(h^r)$ 中求解出 k, r，才能计算出满足 $s = ke + r \pmod q$ 的 e 和 s，而这是一个求解迹函数离散对数难题。而原方案中要想伪造 (A, e)，其困难性在于分解 pq。

在原方案中有两种情况来伪造 (A, e)：

(1)不具有匿名证书的伪造者伪造 (A, e)，只有通过求解出 e 模 $p'q'$ 的逆 $1/e$，然后通过已知的 A, U, Z 伪造 (A, e)。难度相当于分解整数 n。

(2)具有匿名证书的伪造者伪造 (A, e)，同样可用第一种方法来伪造，也可通过计算符合 $m^e = 1 \bmod n$ 的 m 伪造 $A = m\left(\frac{Z}{US^v}\right)^{1/e} \bmod n$，即可伪造出 (A, e)，难度相当于离散对数难题。

而本方案中在不知道证书颁发者私钥的情况下，想伪造匿名证书 (A, e, s)，无论是否具有符合要求的匿名证书，想伪造成功，必须找到满足 $s = ke + r \pmod q$ 的 s 和 e 才能使验证成立，这样必须通过 m 和 n 求得 k, r 才能伪造匿名证书 A, e, s 成功。故伪造难度相当于求解迹函数的离散对数难题。

由此可见，基于 XTR 公钥密码体制的 DAA 方案要比原有的 DAA 方案在安全性方面安全得多。

4.2 完全匿名性分析

本方案是基于现有的 DAA 方案的改进方案，匿名性同原始方案一致。在 DAA 直接匿名认证方案中运用了零知识证明，在申请 DAA 证明阶段隐藏了隐私信息 (f_0, f_1)，验证阶段隐藏了隐私信息 (A, e, s, v)。在申请阶段运用了秘密信息 f 来代替 TPM 的唯一标识 EK 公钥，而且方案中的 DAA 证明只需向颁发者申请一次，且验证者在验证阶段无法获得 (f_0, f_1, A, e, s, v)。

验证者从被认证者 host 发给验证者的签名中分析获得隐私信息 A, e, v 是不可能的，在认证阶段被认证者 host 发给验证者的签名为

$\sigma := (\zeta, (T_1, T_2), N_v, c, n_t, (s_v, s_{f_0}, s_{f_1}, s_e, s_{ee}, s_w, s_{ew}, s_r, s_{er}, s_s))$

式中，$(s_v, s_{f_0}, s_{f_1}, s_e, s_{ee}, s_w, s_{ew}, s_r, s_{er}, s_s)$ 为随机数，每次发送的都不相同，而 (T_1, T_2) 是加入了被认证 host 选取的随机参数 w, r 运算的。由于每次 w, r 随机选择的不同，(T_1, T_2) 的值也都是一个变化的数据。如果验证者想从中获得关于隐私信息，只能从 N_v 中来获得。N_v 是依据 ζ 来计算的，ζ 是通过验证者所提供的基名产生的，而在 TCG 中使用的是变化基名，从而 N_v, ζ 也是变化的。由此可知方案实现了完全匿名性。

4.3 效率分析

本改进方案是基于 XTR 公钥密码体制的，对于 XTR 体制，已知 $Tr(g)$ 和 n，求 $Tr(g^n)$ 的计算量相当于在 $GF(p)$ 中进行 $8\log_2(n)$ 次乘法算法，比 RSA 公钥密码体制中已知 g 和 n，计算 g^n 的运算速度快大约 3 倍。故本改进方案有效地提高了方案的认证运算速度，从而有效地提高了方案的执行效率。此外，因为 $g^n \in GF(p^6)^*$，而 $Tr(g^n) \in GF(p^2)$，所以 $Tr(g^n)$ 的表示、存储、传输所需要的时间、空间复杂度都是 g^n 的 1/3。从而，本方案与原有方案相比，还有效地降低了密钥存储以及传输量。

因此与原基于 RSA 公钥密码体制的 DAA 方案相比，基于 XTR 公钥密码体制改进的 DAA 直接匿名认证方案有效地提高了双方认证效率，提高了安全性，而且密钥存储以及传输量均大大降低。

结束语 针对现有直接匿名认证方案存在的执行效率慢、安全性差等问题，本文结合 XTR 公钥密码体制，在 TCG 规范的基础上，对现有 DAA 方案进行了改进，使得方案的安

全性和认证效率都得到了提高。改进的方案中仍然采用零知识证明的思路。如何有效避免零知识证明的复杂度，进一步提高方案的执行效率，是今后研究的一个方向。

参 考 文 献

[1] Trusted Computing Group. Trusted Computing Group TPM Specification Version1. 2[S]. www. trusted computing group. org. 2003

[2] Brickell E, Camenisch J, Chen L. Direct Anonymous Attestation [C]// The Proceedings of the 11th ACM Conference on Computer and Communications Security. ACM Press, 2004: 132-145

[3] 刘吉强，赵佳，赵勇. 可信计算中远程自动匿名证明的研究[J]. 计算机学报，2009，32(7)：1304-1310

[4] Zhang Fangguo, Chen Xiaofeng, Mu Yi, et al. A New and Efficient Signature on Commitment Values[J]. International Journal of Network Security, 2008, 7(1): 101-106

[5] Chen Xiaofeng, Feng Dengguo. A New Direct Anonymous Attestation Scheme from Bilinear Maps[C]// The Proceedings of 9th International Conference for Young Computer Scientists. 2008: 2308-2313

[6] Brickell E, Chen Liqun, Li Jiangtao. Simplified Security Notions of Direct Anonymous Attestation and a Concrete Scheme from Pairings [J]. International Journal of Information Security, 2009, 8(5): 315-330

[7] Yu Rongwei, Wang Lina, Zhou Yanzhou, et al. An Optimized Anonymous Attestation Protocol from Bilinear Pairing[C]// The Proceedings of 2009 International Conference on Computational Science and Engineering. 2009: 721-726

[8] Lenstra A K, Verheul E R. The XTR public key system[C]// The Proceeding of Crypto2000. LNCS 1880. Spring-Verlag, 2000: 1-19

(上接第 106 页)

C2 =4. 106738302228002e-001

隐藏后左右声道的相关性为：

C3 =4. 106738300576803e-001

从 C1 可以看出隐藏前后左声道的相关性接近 1，说明隐藏信号前后左声道信息几乎无变化。从 C2 和 C3 可以看出，隐藏前后左右声道的相关性大小关系几乎维持不变。

5.3 密钥敏感性测试

本方案对密钥进行了敏感性测试。按以下步骤对 3D-Lorenz 系统初值 $X(0)$ 及可逆矩阵 B 所构成的密钥组中的密钥进行微扰测试。

令舍弃初始迭代次数 $N=5000$。将初始条件 $X(0)$ 及参数 B 进行微扰，产生一维密钥流 $\tilde{c}$，与未扰动时产生的一维密钥流 c 进行比较。取密钥流的长度为 1250010(ASCII 码)。密钥流 $\tilde{c}$ 与 c 对应位的变化个数的百分比如表 1 所列。由表 1 得到 $\tilde{c}$ 与 c 位变化个数的平均值为 99. 600%，非常接近于理想值的 99. 609%(255/256)。由此得出本文的密钥流生成器具有优质的伪随机性功能。

表 1 密钥流 $\tilde{c}$ 与 c 对应的变化个数百分比

密钥扰动	x_1	x_2	x_3	b_{11}	b_{13}	b_{22}	b_{23}	b_{31}	b_{32}	b_{33}	x_1'	x_2'	k
10^{-15}	99. 55	99. 70	99. 50	99. 70	99. 70	99. 55	99. 65	99. 70	99. 70	99. 57	99. 64	99. 68	99. 70
10^{-10}	99. 58	99. 60	99. 63	99. 68	99. 71	99. 60	99. 64	99. 71	99. 65	99. 57	99. 61	99. 64	99. 68
10^{-5}	99. 65	99. 68	99. 70	99. 71	99. 68	99. 58	99. 67	99. 67	99. 69	99. 60	99. 58	99. 65	99. 65
10^{-1}	99. 64	99. 54	99. 65	99. 60	99. 70	99. 59	99. 62	99. 86	99. 69	99. 58	99. 62	99. 63	99. 67

5.4 密钥空间分析

通过对密钥密感性测试的数值模拟表明，本算法对密钥集 keys 来讲，任何试图用微小偏差 10^{-15} 来解密原始文本均是不可能的，因此本方案的密钥空间至少可达到 10^{195}，远大于文献[8]中提到的 10^{45} 个密钥个数。此外，由于设计的同胚函数可以是不计其数的，使得密钥空间足以满足安全通讯的各种要求，对入侵者的强力攻击手段有很强的抵抗能力。

结束语 离散广义混沌同步理论为安全通讯提供了新的工具。本文基于定理和著名的方程构造了一个新的系统，结合 Arnold 猫映射，提出的非对称密钥的音频信息隐藏及语音伪装安全通讯方案具有数据源认证功能和大密钥空间。通过对密钥的敏感性及加密图像相关性分析表明，本方案是一个新型的音频信息隐藏方案，普适性好，为克服时间序列单步预测提供了新思路。

参 考 文 献

[1] 刘海燕，郑雪峰，王颖. 基于 DWT 域乘嵌入音频水印的优化检测算法[J]. 仪器仪表学报，2009，1(30)：148-151

[2] 刘振华，张焕国，叶登攀. 信息隐藏技术及其应用(第二版)[M]. 北京：科学出版社，2009

[3] 张向华. 一种新颖的混沌分组密码算法[J]. 计算机科学，2009，5(36)：92-87

[4] Katzenbeisser S, Petitcclas F A P. 信息隐藏技术-隐写术与数字水印[M]. 吴秋新，钮心忻，杨义先，等译. 北京：人民邮电出版社，2001

[5] 晋建秀，丘水生. 基于物理混沌的混合图像加密系统研究[J]. 物理学报，2010，2(59)：792

[6] Yu Dongchuan, Parlitz U. Partial synchronization of chaotic systems with uncertainty[J]. Phys. Rev. E, 2008, 77(6): 6208

[7] Short K M. Signal extraction from chaotic communications [J]. Int. J. Bifurc. Chaos, 1997, 7(7): 1579-1597

[8] Gao H J, Zhang Y S, Liang S Y. A new chaotic algorithm for image encryption[J]. Chaos Solitons Fractals, 2006, 29: 393

[9] Ji Ye, Liu Ting, Min Lequan. Generalized chaos synchronization theorems for bidirectional differential equations and discrete systems with applications[J]. Physics Letters A, 2008, 372: 3645-3652

[10] Celikovsky S, Chen G R. Secure synchronization of a class of chaotic systems from a nonlinear observe approach[J]. IEEE Trans Autom Control, 2005, 50(1): 76

[11] Min L, Chen G, Zhang X, et al. Approach to generalized synchronization with application to chaos-based secure communication[J]. Commun. Theory Physics, 2004, 41: 632

[12] 臧鸿雁，闵乐泉，吴春雪，等. 基于离散混沌系统广义同步定理的数字图像加密方案[J]. 北京科技大学学报，2007，1：29

[13] Kinzel W, Englert A, Kanter I. On chaos synchronization and secure communication [J]. Phil. Trans. R. Soc. A, 2010, 368 (1911): 379-389