一种基于物理噪声源的复合加密算法

赵和平[1,2], 赵聆波[1]
(1. 中国科学院研究生院 信息安全国家重点实验室, 北京 100049; 2. 中国空间技术研究院, 北京 100094)

摘 要: 为解决短长度航天器测控数据的安全传输问题, 提出了基于物理噪声源、序列密码算法和分组加密算法的复合加密算法 CES; 分析了 CES 算法中物理噪声源、序列密码和分组密码算法的作用; 指出了序列密码给同长度明文的密文长度加熵、物理噪声源给相同明文的密文形式加熵. CES 算法确保了短小指令集传输的安全性并具有安全可靠的认证功能.

关键词: 信息安全; 序列密码; 分组密码; 物理噪声源; 航天器测控
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2009) 10-2193-06

A Combined Encipher System Based on Physical Chaos Generator

ZHAO He-ping[1,2], ZHAO Ling-bo[1]
(1. *State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing* 100049, *China*;
2. *China Academy of Space Technology, Beijing* 100094, *China*)

Abstract: In order to resolve the security problem of the short-length data transmission for spacecraft telecommand and telemetry, a combined encipher system CES, which is based on the physical chaos generator, stream cipher and block ciphers, is proposed in this paper. The effectiveness of the physical chaos generator, stream cipher and block ciphers in the CES were respectively analyzed. The analysis demonstrates that the stream cipher increases the entropy of the length of the cipher-text and the physical chaos generator increases the entropy of the contents of the cipher-text. The CES will insure the security of short-length data transmission and also afford the reliable authentication for the data.

Key words: information security; stream cipher; block cipher; physics chaos generator; spacecraft command and telemetry

1 引言

在航天器测控通讯过程中, 存在大量长度很短且多次重复使用的信息. 例如航天器遥控指令集合的势一般比较小, 指令长度一般也很短. 该类数据的传输问题, 长期以来存在安全隐患. 为解决此问题, 对于数据传输、数据保护的方案、协议、算法已经确定甚至开始使用的已有系统, 可以对待传送的消息先做扩展以增加消息的熵, 再按照常规方法实施数据保护[1,2]. 对于新设计的系统, 本文提出一种基于物理噪声源、序列密码和分组密码算法的复合加密算法 CES. CES 算法借鉴了公开密钥体制中概率加密的思想, 即同 1 个明文可被等概率地加密成多个不同的密文[3~6]. 分析结果表明 CES 算法可以有效增加航天器短消息的密文熵, 对解决该类信息的安全问题是有效和可行的.

2 CES 算法描述

CES 算法由四部分构成:

(1) 序列密码算法 A: 该算法生成序列 $\tilde{b}=\{b_0, b_1, b_2, \cdots\}$, 其中 $b_i \in \{0, 1, 2, \cdots, 2^{n-1}\}$, $i \geqslant 0$, $n \in Z^+$.

(2) 物理噪声源 B: 由其生成序列 $\tilde{r}=\{r_0, r_1, r_2, \cdots\}$, 其中 $r_i \in F_2^p$, $i \geqslant 0$, $p \in Z^+$, 一般 p 为 128 比特或 256 比特.

(3) 加密算法 $\overline{E}_k$ 为 p 比特的分组密码算法(其解密算法为 $\overline{D}_k$);

(4) 加密算法 E_k 为 p 比特的分组密码算法(其解密算法为 D_k).

不失一般性, 可以给出如下函数:

$$s(b_i)=\begin{cases} n_0, & b_i=0 \\ n_1, & b_i=1 \\ \vdots & \\ n_{2^n-1}, & b_i=2^{n-1} \end{cases},$$

其中 $0<n_0<n_1<\cdots<n_{2^n-1}$.

对于明文序列 $\tilde{a}=\{a_0, a_1, a_2, \cdots\}$, $a_i \in F_2^p$, 加密过程如下:

收稿日期: 2007-08-17; 修回日期: 2009-08-01
基金项目: 国家 863 高技术研究发展计划(No. 2004AA741071)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

(1) 利用序列密码算法 A 产生的序列 $\tilde{b}$ 确定对应于每一明文分组 a_i 的 $s(b_i)$, 则其对应的密文长度为 $[s(b_i)+1]p$ 比特; 以物理噪声源 B 产生的序列 $\tilde{r}$ 和分组密码算法 $\bar{E}_{\bar{k}}$ 对明文序列 $\tilde{a}$ 中的明文分组 a_i 做如下变换:

$$M_i = r_{l_i} r_{l_i+1} \cdots r_{l_i+s(b_i)-1} f_{s(b_i)}(r_{l_i}, r_{l_i+1}, \cdots, r_{l_i+s(b_i)-1}, a_i)$$

其中 $l_0 = 0$, $l_i = \sum_{j=0}^{i-1} s(b_j)$, $i > 0$, 函数

$$f_{s(b_i)}(r_{l_i}, r_{l_i+1}, \cdots, r_{l_i+s(b_i)-1}, a_i) = \bar{E}_{\bar{k}}(r_{l_i}) \oplus \cdots \oplus \bar{E}_{\bar{k}}(r_{l_i+s(b_i)-1}) \oplus \bar{D}_{\bar{k}}(a_i).$$

(2) 用加密算法 E_k 作用 M_i 得到密文段:

$$c_i = E_k(r_{l_i}) E_k(r_{l_i+1}) \cdots E_k(r_{l_i+s(b_i)-1}) \cdot E_k(f_{s(b_i)}(r_{l_i}, r_{l_i+1}, \cdots, r_{l_i+s(b_i)-1}, a_i))$$

从而可得到密文序列 $\tilde{c} = \{c_0, c_1, c_2, \cdots\}$.

解密过程如下:

(1) 利用序列密码算法 A 产生的序列 $\tilde{b}$ 得到 $s(b_i)$, 确定每一组密文 c_i 的长度 $[s(b_i)+1]p$ 比特, 对密文序列 $\tilde{c}$ 定界, 得到 c_i, $i \geqslant 0$.

(2) 用解密算法 D_k 作用于 c_i, 得:

$$D_k(E_k(r_{l_i})) \cdots D_k(E_k(r_{l_i+s(b_i)-1})) \cdot D_k(E_k(f_{s(b_i)}(r_{l_i}, r_{l_i+1}, \cdots, r_{l_i+s(b_i)-1}, a_i)))$$
$$= r_{l_i} r_{l_i+1} \cdots r_{l_i+s(b_i)-1} f_{s(b_i)}(r_{l_i}, r_{l_i+1}, \cdots, r_{l_i+s(b_i)-1}, a_i)$$
$$= M_i.$$

(3) 由上步已求出的 $r_{l_i}, r_{l_i+1}, \cdots, r_{l_i+s(b_i)-1}$, 可以求出 $\bar{E}_{\bar{k}}(r_{l_i}) \oplus \cdots \oplus \bar{E}_{\bar{k}}(r_{l_i+s(b_i)-1})$, 进而由 $f_{s(b_i)}$ 解出 a_i, $i \geqslant 0$.

$$\bar{E}_{\bar{k}}(r_{l_i}) \oplus \cdots \oplus \bar{E}_{\bar{k}}(r_{l_i+s(b_i)-1}) \oplus f_{s(b_i)}(r_{l_i}, r_{l_i+1}, \cdots, r_{l_i+s(b_i)-1}, a_i)$$
$$= \bar{E}_{\bar{k}}(r_{l_i}) \oplus \cdots \oplus \bar{E}_{\bar{k}}(r_{l_i+s(b_i)-1}) \oplus \bar{E}_{\bar{k}}(r_{l_i}) \oplus \cdots \oplus \bar{E}_{\bar{k}}(r_{l_i+s(b_i)-1}) \oplus \bar{D}_{\bar{k}}(a_i) = \bar{D}_{\bar{k}}(a_i).$$

则 $\bar{E}_{\bar{k}}(\bar{D}_{\bar{k}}(a_i)) = a_i$.

(4) 重复步骤(2)和(3), 直到解出全部明文序列 $\tilde{a} = \{a_0, a_1, a_2, \cdots\}$.

以 $n = 2$、$s(b_i) = \begin{cases} 1, & b_i = (00) = 0 \\ 2, & b_i = (01) = 1 \\ 3, & b_i = (10) = 2 \\ 4, & b_i = (11) = 3 \end{cases}$,

$\tilde{b} = \{b_0, b_1, b_2, b_3, \cdots\} = \{01, 10, 11, 00, \cdots\}$, 明文序列 $\tilde{a} = \{a_0, a_1, a_2, a_3, \cdots\}$, $a_i \in F_2^p$ 为例, CES 加密过程如下:

(1) 构造 $\tilde{M} = \{M_0, M_1, M_2, M_3, \cdots\}$:

$$M_0 = r_0 r_1 f_2(r_0, r_1, a_0) = r_0 r_1 [\bar{E}_{\bar{k}}(r_0) \oplus \bar{E}_{\bar{k}}(r_1) \oplus \bar{D}_{\bar{k}}(a_0)],$$
$$M_1 = r_2 r_3 r_4 f_3(r_2, r_3, r_4, a_1) = r_2 r_3 r_4 [\bar{E}_{\bar{k}}(r_2) \oplus \bar{E}_{\bar{k}}(r_3) \oplus \bar{E}_{\bar{k}}(r_4) \oplus \bar{D}_{\bar{k}}(a_1)],$$
$$M_2 = r_5 r_6 r_7 r_8 f_4(r_5, r_6, r_7, r_8, a_2) = r_5 r_6 r_7 r_8 [\bar{E}_{\bar{k}}(r_5) \oplus \bar{E}_{\bar{k}}(r_6) \oplus \bar{E}_{\bar{k}}(r_7) \oplus \bar{E}_{\bar{k}}(r_8) \oplus \bar{D}_{\bar{k}}(a_2)],$$
$$M_3 = r_9 f_1(r_9, a_3) = r_9 [\bar{E}_{\bar{k}}(r_9) \oplus \bar{D}_{\bar{k}}(a_3)], \cdots\cdots$$

(2) 得到密文 $\tilde{c} = \{c_0, c_1, c_2, c_3, \cdots\}$, 其中:

$$c_0 = E_k(r_0) E_k(r_1) E_k(\bar{E}_{\bar{k}}(r_0) \oplus \bar{E}_{\bar{k}}(r_1) \oplus \bar{D}_{\bar{k}}(a_0)),$$
$$c_1 = E_k(r_2) E_k(r_3) E_k(r_4) E_k(\bar{E}_{\bar{k}}(r_2) \oplus \bar{E}_{\bar{k}}(r_3) \oplus \bar{E}_{\bar{k}}(r_4) \oplus \bar{D}_{\bar{k}}(a_1)),$$
$$c_2 = E_k(r_5) E_k(r_6) E_k(r_7) E_k(r_8) E_k(\bar{E}_{\bar{k}}(r_5) \oplus \bar{E}_{\bar{k}}(r_6) \oplus \bar{E}_{\bar{k}}(r_7) \oplus \bar{E}_{\bar{k}}(r_8) \oplus \bar{D}_{\bar{k}}(a_2)),$$
$$c_3 = E_k(r_9) E_k(\bar{E}_{\bar{k}}(r_9) \oplus \bar{D}_{\bar{k}}(a_3)), \cdots\cdots$$

相应的解密过程如下:

(1) 利用序列 $\tilde{b}$ 对密文序列 $\tilde{c}$ 定界, 得到 c_i.

(2) 用解密算法 D_k 作用 $\tilde{c} = \{c_0, c_1, c_2, c_3, \cdots\}$:

$$D_k(E_k(r_0)) D_k(E_k(r_1)) D_k(E_k(\bar{E}_{\bar{k}}(r_0) \oplus \bar{E}_{\bar{k}}(r_1) \oplus \bar{D}_{\bar{k}}(a_0)))$$
$$= r_0 r_1 f_2(r_0, r_1, a_0) = M_0,$$
$$D_k(E_k(r_2)) D_k(E_k(r_3)) D_k(E_k(r_4)) D_k(E_k(\bar{E}_{\bar{k}}(r_2) \oplus \bar{E}_{\bar{k}}(r_3) \oplus \bar{E}_{\bar{k}}(r_4) \oplus \bar{D}_{\bar{k}}(a_1)))$$
$$= r_2 r_3 r_4 f_3(r_2, r_3, r_4, a_1) = M_1,$$
$$D_k(E_k(r_5)) D_k(E_k(r_6)) D_k(E_k(r_7)) D_k(E_k(r_8)) D_k(E_k(\bar{E}_{\bar{k}}(r_5) \oplus \bar{E}_{\bar{k}}(r_6) \oplus \bar{E}_{\bar{k}}(r_7) \oplus \bar{E}_{\bar{k}}(r_8) \oplus \bar{D}_{\bar{k}}(a_2)))$$
$$= r_5 r_6 r_7 r_8 f_4(r_5, r_6, r_7, r_8, a_2) = M_2,$$
$$D_k(E_k(r_9)) D_k(E_k(\bar{E}_{\bar{k}}(r_9) \oplus \bar{D}_{\bar{k}}(a_3)))$$
$$= r_9 f_1(r_9, a_3) = M_3.$$

(3) 由 $f_{s(b_i)}$ 解出 a_i, $i \geqslant 0$.

因为由上步已求出 $r_0, r_1, \cdots, r_9$, 故可求出:

$[\bar{E}_{\bar{k}}(r_0) \oplus \bar{E}_{\bar{k}}(r_1)]$, $[\bar{E}_{\bar{k}}(r_2) \oplus \bar{E}_{\bar{k}}(r_3) \oplus \bar{E}_{\bar{k}}(r_4)]$, $[\bar{E}_{\bar{k}}(r_5) \oplus \bar{E}_{\bar{k}}(r_6) \oplus \bar{E}_{\bar{k}}(r_7) \oplus \bar{E}_{\bar{k}}(r_8)]$, $\bar{E}_{\bar{k}}(r_9)$, ……从而

$$\bar{E}_{\bar{k}}(\bar{D}_{\bar{k}}(a_0)) = a_0,$$
$$\bar{E}_{\bar{k}}(\bar{D}_{\bar{k}}(a_1)) = a_1,$$
$$\bar{E}_{\bar{k}}(\bar{D}_{\bar{k}}(a_2)) = a_2,$$
$$\bar{E}_{\bar{k}}(\bar{D}_{\bar{k}}(a_3)) = a_3, \cdots\cdots$$

(4) 最后得明文序列 $\tilde{a} = \{a_0, a_1, a_2, a_3, \cdots\}$.

3 序列密码的作用分析

传统意义下, 当明文长度固定时密文长度的熵为零. CES 算法中, 序列密码算法的作用是给密文长度加熵, 随着控制位 n 的增加, 密文长度的熵增大. 下面给出理论分析.

定义 1 设序列 $\tilde{d} = \{d_0, d_1, d_2, \cdots\} \in F_2^p$, 定义右移算子 R^l 为:

$$R^l(\tilde{d}) = \overbrace{0 \cdots 0}^{l\text{个}} d_0 d_1 d_2 \cdots,$$

其中 $0 = \overbrace{(0, \cdots, 0)}^{p\text{个}} \in F_2^p$.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net