基于国密算法的无人机保密通信

杜 爽[1] 霍思羽[1] 王永强[1] 丁 辉[1]
DU Shuang HUO Siyu WANG Yongqiang DING Hui

摘 要 随着无人机技术的快速迭代升级，其在农作物经济、应急救援、娱乐活动、物流运输等低空领域的应用日益广泛。不同应用场景对通信安全的需求存在显著差异，农作物浇灌、娱乐活动等场景对通信安全性要求相对较低，而应急救援等场景则对通信安全有着极高要求。为保障无人机在通信过程中免遭恶意攻击，加密算法的应用至关重要。文章提出了一种基于国密算法 SM2 与 SM4 相结合的保密通信方式，通过深入研究与实践验证，成功实现了无人机与地面控制站之间的安全通信，有效提升了无人机通信系统的安全性与可靠性，为无人机在高安全需求场景下的应用提供了有力的技术支撑。

关键词 无人机；保密通信；SM2；SM4

doi：10.3969/j.issn.1672-9528.2025.06.026

0 引言

无人机是一种未搭载飞行员的遥控或者计算机程序辅助飞行器[1]，具有体积小、灵敏、运动空间大等优点，广泛应用在各个行业领域中。但是，无人机暴露在公共网络中，容易遭到恶意攻击。随之带来的隐私安全问题不容忽视。一些典型的攻击，比如非法窃听信息、拒绝服务攻击、重放攻击等[2]，会造成重要信息泄露，飞行任务失败。甚至会通过单个无人机节点威胁到整个无人机网络的信息安全。在无人机网络通信中，密码算法的应用可以保障无人机安全通信、安全飞行。

在现代密码学中，密码算法分为对称算法、非对称算法。对称算法运行速率快，但加解密依赖于同一个密钥。当密钥丢失，会造成信息泄露。非对称算法的协商体制，能够每次协商出新的会话密钥。对称算法与非对称算法的结合运用，既能保证高效率加解密，又能保证加解密密钥的按需更新。RSA 算法作为一种经典的非对称算法，是基于大数分解问题的复杂性来实现加密安全的，但其运行效率相对较低。为了提高性能，密码学领域不断开拓新的协商算法。作为我国自主研发的国密算法 SM2 中的密钥协商体制，充分利用了椭圆曲线上离散对数计算的独特优势，确保其安全性和可信度。SM2 算法相比于国际上通用的 RSA 算法[3]、ECC[4] 算法，在同等安全的情况下效率更高[5]。目前国密算法 SM4[6-7] 作为对称算法中的分组算法，相对于国际通用的 3DES 算法[8] 具有更高的安全性。因此，本文结合国密算法 SM2 和 SM4 实现无人机的保密通信。

1 无人机通信安全需求

无人机通信系统由地面控制站与无人机组两部分构成，如图 1 所示。

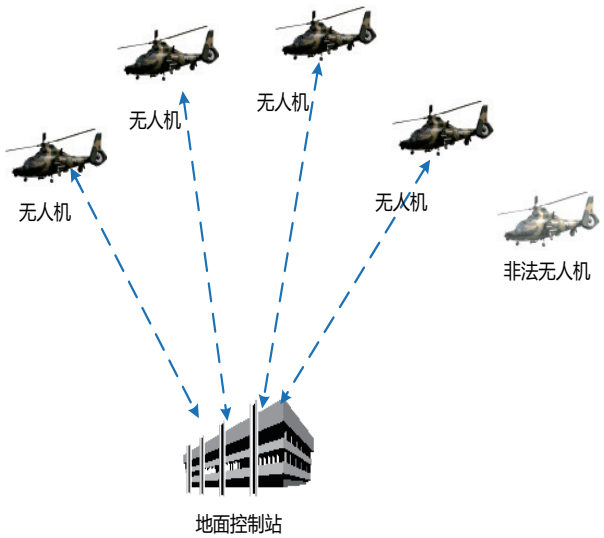

图 1 地面控制站与无人机组通信图

地面控制站可以通过指令控制无人机的运行轨迹，无人机上所安装的传感器也可以将采集到的信息反馈到地面控制站。当地面控制站与无人机组的通信采用明文方式传输信息时，非法无人机可以窃听并篡改中心站对无人机的控制指令，会影响任务的顺利进行。同时，非法无人机也可以窃听无人机发送给中心站的信息，造成重要数据泄露。因此，整个链路的双向通信需要重点解决两方面的信息安全需求。

1. 中国电子科技集团公司第三十研究所 四川成都 610041

（1）保密性，确保通信数据在传输过程中不会泄露给非法无人机。

（2）完整性，确保通信数据在传输过程中不会被非法无人机篡改。

2 方案设计

为保证地面控制站与无人机之间的安全通信，本文采用国密算法 SM2 和国密算法 SM4 组合方式。首先采用 SM2 椭圆曲线协商算法，生成各自的会话密钥。然后再采用 SM4 分组算法的 CBC 模式与刚协商出来的会话密钥对通信进行加解密。由于椭圆曲线协商算法运行效率相对较低，不需要实时去更新会话密钥。在安全性与加解密速率兼顾的同时，采用定时协商的方式，按需更新会话密钥。这种方式，既保证了加解密密钥的前向安全性，也保证了通信过程中的加解密速率。

2.1 SM4 算法设计

SM4 算法工作原理为输入明文的一个分组为 16 Byte，以 4 个字 X_0、X_1、X_2、X_3 表示。将 X_0、X_1、X_2、X_3 作为输入，在轮密钥 rk_0 的参与下，通过轮函数运算生成 X_1、X_2、X_3、X_4。然后将 X_1、X_2、X_3、X_4 作为输入，在轮密钥 rk_1 的参与下，通过轮函数生成 X_2、X_3、X_4、X_5。依次迭代，经过 32 次轮函数运算生成 X_{32}、X_{33}、X_{34}、X_{35}。最后将 4 个字反序获得密文，如图 2 所示。

$$(Y_0, Y_1, Y_2, Y_3) = (X_{35}, X_{34}, X_{33}, X_{32})$$

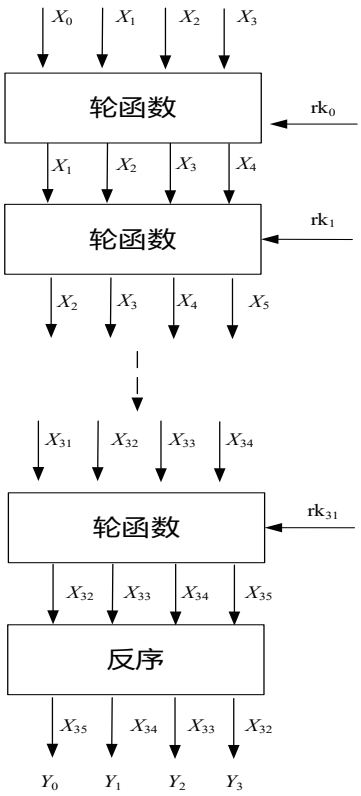

图 2 SM4 算法工作原理

加密过程中的轮函数的操作流程如图 3 所示，轮函数的计算公式为：

$$X_{i+4} = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus \mathrm{rk}_i) \quad (1)$$

输入明文 X_{i+1}、X_{i+2}、X_{i+3} 与轮密钥 rk_i 异或生成后的数据作为合成置换 T 模块的输入，输出结果再与 X_i 异或生成新的 X_{i+4}。

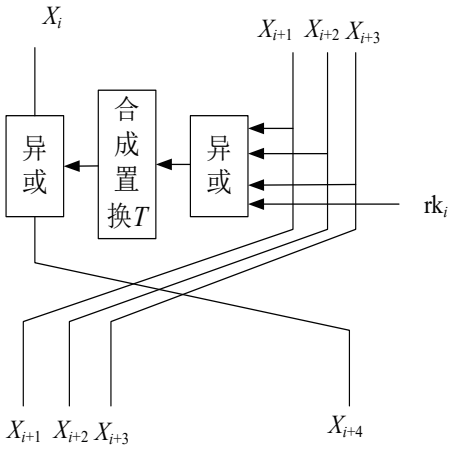

图 3 轮函数生成原理

加密过程中的轮密钥是通过初始化向量 $\boldsymbol{M}_K$ 派生而来。在 32 次迭代运算中，每轮运算都需要一个轮密钥参与。因此，需要将初始化向量 $\boldsymbol{M}_K$ 通过一系列运算生成 32 个轮密钥。初始化向量 $\boldsymbol{M}_K$ 为 16 Byte，以 4 字 $\boldsymbol{M}_{K0}$、$\boldsymbol{M}_{K1}$、$\boldsymbol{M}_{K2}$、$\boldsymbol{M}_{K3}$ 表示。则轮密钥 rk_i（i=0, 1, 2, …, 31）的计算公式为：

$$(K_0, K_1, K_2, K_3) = (\boldsymbol{M}_{K0} \oplus F_{K0}, \boldsymbol{M}_{K1} \oplus F_{K1}, \boldsymbol{M}_{K2} \oplus F_{K2}, \boldsymbol{M}_{K3} \oplus F_{K3}) \quad (2)$$

$$\mathrm{rk}_i = K_{i+4} = K_i \oplus T'(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus C_{Ki}) \quad (3)$$

式中：F_K 为系统参数；C_K 为固定参数。参数 F_K、C_K 均以字参与上述运算。

SM4 加密算法具有多种工作模式，包括 ECB、GCM、CBC 等。ECB 是最简单的加密模式，将明文划分为独立的 128 位分组，对每个分组进行独立运算。这种加密方式安全性较低，相同的加密模块会被加密成相同的密文，容易被攻击者识别。GCM 提供了加密和认证功能，安全性极高，但是复杂度高，处理时间相对较长，并不适用于加解密效率要求高的场景。CBC 通过引入链式依赖来提高安全性，每个分组依赖于前一个分组。因此即使是完全相同的明文也有可能会有完全不同的密文输出。相比于 ECB 模式，CBC 模式具有更高的安全性和抗攻击性。相比于 GCM 模式，CBC 模式的运行效率相对较高。综合考虑，本文采用 SM4 算法的 CBC 模式。SM4 算法的 CBC 模式的加密流程如图 4 所示，解密流程如图 5 所示。

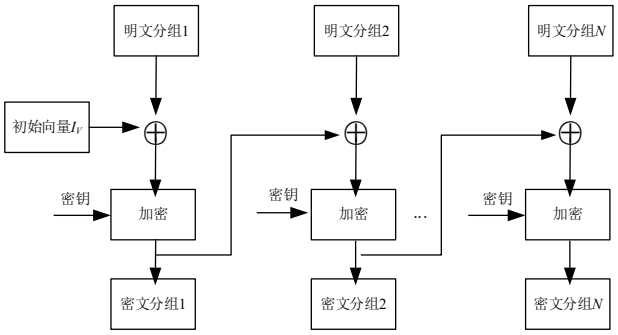

图 4 SM4 算法 CBC 模式加密流程图

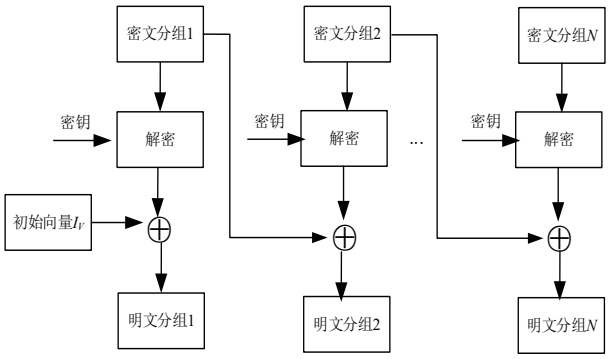

图 5 SM4 算法 CBC 模式解密流程图

在无人机与地面控制站通信过程中，加密方首先通过随机数模块产生 16 Byte 初始化向量 $\boldsymbol{I}_V$，第一个分组的明文与初始化向量 $\boldsymbol{I}_V$ 异或后的结果通过加密模块进行加密可获得第一个分组密文。然后，第二个分组明文与第一个分组密文进行异或后的结果，经由加密模块进行加密生成第二个分组密文。以此类推，可获得所有分组的密文。最后加密方将拼接好的密文与初始化向量 $\boldsymbol{I}_V$ 一起发送给解密方。

在解密过程中，解密方将第一个分组密文经由解密模块运算后的结果与初始化向量 $\boldsymbol{I}_V$ 异或生成第一个分组密文。然后，第二个分组密文经由解密模块运算后的结果与第一个分组密文进行异或生成第二个分组的明文。以此类推，可获得所有分组的明文。最后，将所有分组的明文拼接成完整的明文数据即可。

2.2 SM2 算法协商设计

地面控制站与无人机组构成的通信系统的运行主要分为 3 个阶段：部署阶段、协商阶段、通信阶段。

在部署阶段，地面控制站生成控制站与无人机的关键信息，并将控制站信息存储在本地，无人机信息发送给无人机。在协商阶段，通过非对称算法 SM2 的一系列运算，以及关键信息生成会话密钥。在通信阶段，采用分组算法 SM4 的 CBC 模式，以及协商出来的会话密钥共同实现地面控制站与无人机的保密通信。从部署到实现加解密通信过程如图 6 所示。

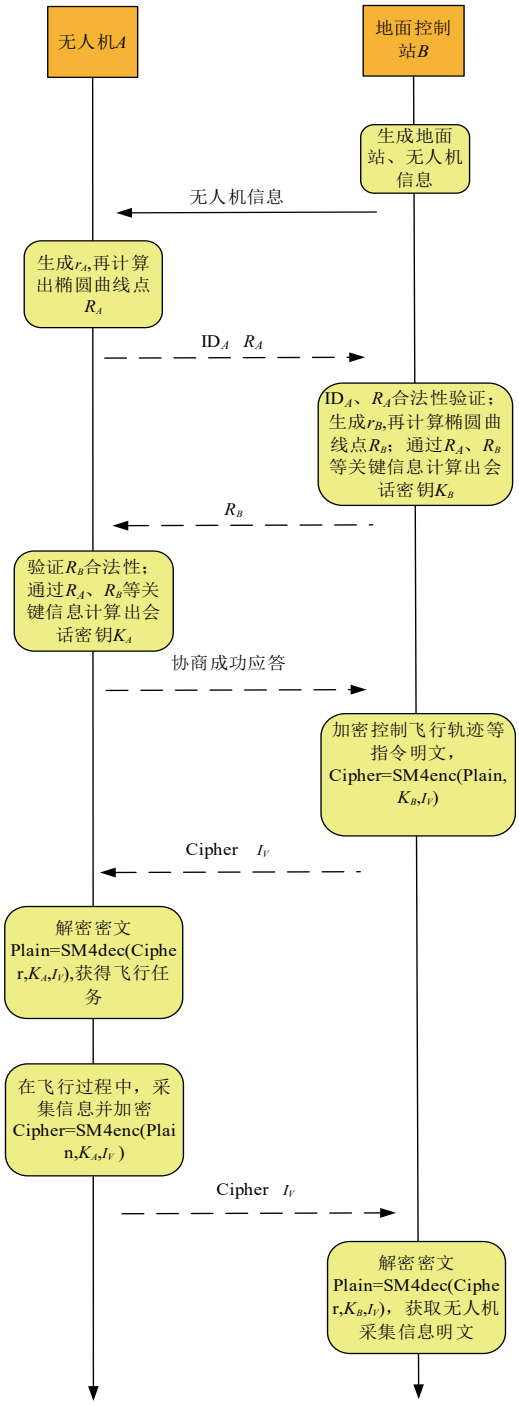

图 6 地面控制站与无人机通信流程示意图

2.2.1 部署阶段

在无人机起飞前，地面控制站需要生成控制站和无人机信息。

SM2 椭圆曲线用公式表示为：

$$y = x + ax + b(\mathrm{mod}\ p) \tag{4}$$

式中：$a, b \in F_p$。

假设 $G=(x_g, y_g)$ 为椭圆曲线基点，G 的阶为 n。首先生成控制站的身份 ID_B、公钥 P_B、私钥 d_B。然后通过哈希运算获

得关键信息的摘要值，公式为：

$$Z_B = \mathrm{hash}(\mathrm{ENTL}_B \| \mathrm{ID}_B \| a \| b \| x_G \| y_G \| x_B \| y_B) \quad (5)$$

式中：ENTL_B 为 ID_B 长度。

后生成无人机的身份 ID_A、公钥 P_A、私钥 d_A，并通过哈希运算获得关键信息的摘要值 Z_A。

最后将$(d_B, P_B, \mathrm{ID}_B, Z_B, P_A, \mathrm{ID}_A, Z_A, G, n)$存储在本地。将$(d_A, P_A, \mathrm{ID}_A, Z_A, P_B, Z_B, G, n)$通过有线网络分发给无人机。

2.2.2 协商阶段

（1）起飞后，由无人机主动建立连接，发起协商申请。无人机运算单元生成随机数 r_A，然后计算椭圆曲线点 R_A，将 ID_A、R_A 通过无线网络发送给控制站。

（2）控制站收到来自无人机的信息后，先判断 ID_A 的合法性，然后判断 R_A 是否在椭圆曲线点上。其中任何一个资源错误都终止协商流程。合法性验证通过后，控制站运算单元产生随机数 r_B，然后计算椭圆曲线点 R_B。分别从 R_B、R_A 中提取域元素经过计算获得 V。若 V 为无穷点则协商失败。否则，可计算出会话公钥 K_B。计算公式为：

$$K_B = \mathrm{KDF}(x_V \| y_V \| Z_B \| Z_A, \mathrm{klen}) \quad (6)$$

将 R_B 发送给无人机。

（3）无人机收到控制站的信息后，先判断 R_B 是否在椭圆曲线点上。若不是，终止协商流程；若是，分别从 R_A、R_B 中提取域元素经过计算获得 V。若 V 为无穷点则协商失败；否则，可计算出会话公钥 K_A。

2.2.3 通信阶段

采用 2.1 章节描述的 SM4 分组算法的 CBC 模式，密钥为协商出来的会话密钥 K_A、K_B，对通信数据进行加解密。

当地面控制站需要无人机执行任务时，首先，通过随机数模块生成初始化向量 $\boldsymbol{I}_V$，采用 SM4 算法的 CBC 模式，加密密钥为 K_B，将无人机的运行轨迹、目标信息等数据进行加密获得密文；然后，地面控制站将密文、$\boldsymbol{I}_V$ 无线发送给无人机，无人机收到来自地面控制站的密文数据后，采用 SM4 算法的 CBC 模式，解密密钥为 K_A，初始化向量为 $\boldsymbol{I}_V$，对密文数据进行解密运算获得明文；最后，无人机就可以根据地面控制站发布的运动轨迹与目标地等信息执行飞行任务。

在执行侦察任务时，无人机会将飞行过程中采集到的信息发送给地面控制站。首先，无人机通过随机数模块生成初始化向量 $\boldsymbol{I}_V$；接着，采用 SM4 算法的 CBC 模式，加密密钥为 K_A，将采集到的信息加密成密文；然后，无人机将密文、$\boldsymbol{I}_V$ 无线发送给地面控制站，当地面控制站收到来自无人机的密文信息后，采用 SM4 算法的 CBC 模式，解密密钥为 K_B，初始化向量为 $\boldsymbol{I}_V$，将密文解密生成明文；最后，地面控制站就能获得无人机的侦察信息。

在双方通信过程中，SM4 分组算法与 SM2 协商算法相结合，共同保障敏感信息不被非法窃听与篡改。

3 结语

本文采用了 SM4 分组算法和 SM2 协商算法相结合的架构，解决了地面控制站与无人机通信安全问题。这种通信方式能通过协商的方式按需更换会话密钥，保证了密钥前向安全性。采用分组算法 SM4 加解密，运行速率高，能实时传输通讯数据。这种双算法结合方式在保证加解密速率的同时，具有更强的安全性，可以抵御假冒攻击、中间人攻击、重放攻击等多种非法攻击。

参考文献：

[1] 王杰华 . 面向无人机网络的通信隐私保护方案研究与设计 [D]. 成都 : 电子科技大学 ,2023.

[2] 吕龙伟 . 轻量级无人机网络安全通信协议 [D]. 西安 : 西安电子科技大学 , 2020.

[3] GONG L H, QIU K D, DENG C Z, et al. An optical image compression and encryption scheme based on compressive sensing and RSA algorithm[J].Optics and lasers in engineriong, 2019, 121: 169-180.

[4] VERMA O P, JAIN N, PAL S K. Design and analysis of sn aptimal ECC algorithm with affective access control mechanism for big data[J]. Multimedia tools and applications, 2020, 79: 9757-9783.

[5] 郭锐 . 基于国密算法的轻量级无人机网络认证密钥协商协议设计 [D]. 西安 : 西安电子科技大学 , 2021.

[6] GNational information security standardization technical committee. Information security technology-SM4 block cipher algorithm: GB/T 32907-2016[S].Beijing: Standards press of China, 2016.

[7] 罗晓蝶 . 基于轻量级国密 SM4 算法的安全加密认证 IP 核设计 [D]. 武汉 : 湖北大学 ,2023.

[8] ZHAO Y Q, LI Q J, GU Z. Early smoke detection of forest fire video using CS adaboost algorithm[J].Optik-international journal for light and electron optics, 2015,126(19): 2021-2124.

【作者简介】

杜爽（1990—），女，硕士研究生，工程师，研究方向：信息安全与保密通信、嵌入式软件开发。

霍思羽（1991—），女，硕士研究生，工程师，研究方向：信息安全、嵌入式软件设计。

王永强（1994—），男，硕士研究生，工程师，研究方向：保密通信、嵌入式软件设计。

丁辉（1993—），男，硕士研究生，工程师，研究方向：保密通信、嵌入式软件开发。

（收稿日期：2025-01-14 修回日期：2025-05-10）