Vol.2019-CSEC-86 No.10
Vol.2019-SPT-34 No.10
2019/7/23

観測ロケットMOMO3号機による小型衛星・小型ロケット用セキュア通信方式の基礎実験

吉田 真紀[1]　森岡 澄夫[2]　尾花 賢[3]

概要：平成 30 年 11 月 15 日に人工衛星等の打上げ及び人工衛星の管理に関する法律が施行された．同法律に関するガイドラインには，人工衛星の打上げ用ロケットとの通信に際してセキュリティ確保が必要であることが明記されている．民間事業者が宇宙ビジネスに参入する新たな時代に向け，著者らはこれまでに，小型衛星・小型ロケット用セキュア通信のためのセキュリティモデルを定め，情報理論的安全な方式を提案するとともに，プロトタイプ実装および地上での評価実験を行い，理論上最高レベルの安全性が低コストで達成できうることを示してきた．本稿では，提案方式の実験用回路を観測ロケット MOMO3 号機に搭載し動作確認した結果を報告する．本実験で，提案するセキュリティ機構が飛行時環境の下で正常に動作することを確認し，実用化に向けた肯定的結果が得られた．

キーワード：小型衛星，小型ロケット，通信セキュリティ，情報理論的安全性，飛行実験

Preliminary Experiment of Secure Communication on Sounding Rocket MOMO-3

Maki Yoshida[1]　Sumio Morioka[2]　Satoshi Obana[3]

1. はじめに

小型衛星が学術・商用目的で多数打ち上げられるようになり，今後も急激に数が増加していくことが見込まれている [23]．それに伴い，小型衛星打上げ専用の低コスト小型ロケットが開発されるようになり [9]，平成 30 年 11 月 15 日，人工衛星等の打上げ及び人工衛星の管理に関する法律 (いわゆる宇宙活動法) も施行された．

宇宙活動法に関する諸ガイドラインには，人工衛星の打上げ用ロケットの型式認定や飛行許可にあたって，重要なシステム等に関する信号の送受信については，適切な暗号化等の措置が求められる旨が記載されている [21], [22]．実際，重要なシステム等に関する信号には飛行中断などクリティカルなコマンドが含まれており，公共の安全を脅かさないためにも，第三者による成りすましやコマンド改ざんを受けてはならない．それ以外の信号の送受信においても，学術・商用的に高い価値を有する衛星から地上への伝送データが盗聴されることは好ましくない．

著者らは，民間事業者が宇宙ビジネスに参入する新たな時代に向け，小型衛星・小型ロケット用セキュア通信技術の研究開発に取り組んでいる [18], [20]．文献 [20] ではまず，小型衛星・小型ロケットとの通信における固有の特徴と課題を抽出し，求められるセキュリティ要件を整理した．そして，情報理論的安全性の実現可能性に主眼をおき，地上局と小型衛星・小型ロケット間が通信を行う期間における総通信量を分析した．その結果，現在衛星やロケットに搭載可能な低コスト電子デバイスを用いて情報理論的安全

[1] 情報通信研究機構, 東京都小金井市貫井北町 4-2-1, NICT, 4-2-1 Nukuikitamachi, Koganei, Tokyo, Japan
[2] インターステラテクノロジズ, 千葉県浦安市北栄 4-28-21, Interstellar Technologies, 4-28-21 Kitazakae, Urayasu, Chiba, Japan
[3] 法政大学, 東京都小金井市梶野町 3-7-2, Hosei University, 3-7-2 Kajinocho, Koganei, Tokyo, Japan

性が実現できることを見出し，方式を提案した．文献 [20] では，提案方式の主要セキュリティ機構をプロトタイプ実装し，地上での評価実験を実施して有効性を確認すると共に，対象システム固有の特徴と課題を具体化した．その結果を踏まえ，セキュリティモデルを定め，[20] で提案した方式の安全性証明を与えている．

本稿では，提案方式の主要セキュリティ機構の実験用回路を観測ロケット MOMO3 号機 [*1]に搭載し，2019 年 5 月 4 日に打上げ，動作確認した結果を報告する．実験の結果，情報理論的安全な方式が計算量的安全な方式より適していること，および提案するセキュリティ機構が飛行時環境の下で正常に動作することを確認し，実用化に向けた肯定的結果が得られた．

2. 小型衛星・小型ロケット用通信における課題

本研究で対象とする通信システムにおけるエンティティは，地上局，小型ロケット，小型衛星，測位衛星の四つである．

文献 [20] における検討で，測位衛星からは基本的には受信のみ，主な通信は地上局と小型ロケット・小型衛星との無線通信，求められるセキュリティ要件は，セキュリティの基本要件である秘匿，認証，可用性であることを明らかにした．秘匿，認証，可用性は，従来の地上通信システムでも考えられている．

そこで，対象とする通信システム固有の課題を検討した．まず，地上局にとって通信相手であり制御相手である小型ロケットが打上げ数分後には音速の数倍以上という高速で移動する．そのため，セキュリティ関連処理による遅延は，状況変化への対応の遅れに直結し，公共の安全性を著しく損なう可能性がある．よって，簡単な演算からなる軽量な暗号技術を利用すべきである．

さらに，管制情報・ミッションデータの改ざんや送信元のなりすましは，飛行中断・継続コントロールを含むミッション遂行を不能にするため，能動的な攻撃への高いセキュリティの達成が重要になる．

能動的攻撃への一般的な対策として，対策 1) Bulletin board [4], [6], 対策 2) Common reference string [3], [5], [8], 対策 3) Interaction が知られている．しかし，対策 1) については，地上局と小型ロケット・小型衛星との通信周波数は一般に機密情報であり，無線処理系は局外との通信系からは分離されているため，誰もが読み書きできる公開の Bulletin board は使えない．次に，対策 2) として，測位衛星の信号から得られる時刻情報を Common reference string とすることが考えられるが，処理装置における精度等に依存して，地上局と小型ロケット・小型衛星との間で時刻ずれが発生しうる．お互いの情報を確認するために，対策 3) の Interaction を許すと，通信が安定しない状況でやりとりの齟齬から管制を喪失する可能性がある．信頼できる時刻情報として，高精度オシレータを搭載し，打上げ前に地上局と小型ロケット・小型衛星で時刻合わせをすることが考えられるが，現在利用可能な高精度オシレータ (OCXO や TCXO) でも 1 日で数ミリ秒のずれが生じうるため，数ヶ月〜数年に渡って周回する小型衛星では十分ではない．

また，飛行環境に起因するデータ破損が生じうるため，対策の検討を進める上で飛行環境下における演算回路やストレージなどの構成部品の信頼性評価が不可欠であり，それを踏まえたシステムとしての高信頼性の達成が重要である．

すなわち，対象とする通信システムでは，地上局と小型ロケット・小型衛星との間で時刻ずれが発生する状況でインタラクションを可能な限り排除し，要件 1) 計算効率が良く回路規模が小さい，要件 2) 高セキュリティ，要件 3) 低コスト，要件 4) 高信頼な実装方式を設計する必要がある．

文献 [20] では，要件 1)〜3) を満たす非対話な方式を提案した．まず，要件 1) と 2) は，計算効率が良く回路規模が小さい，かつ情報理論的安全な暗号方式を利用することで満たした．情報理論的安全な暗号方式では大量の使い捨て鍵の事前共有が必要になるため，従来の地上通信システムの構築においては利用されていない．それに対して，対象とする通信システムは， 打ち上げ前に地上局と小型ロケット・小型衛星が物理的に近接するため鍵共有が容易であり，ライフタイムが比較的短く総通信量が抑えられる．これらにより，情報理論的安全性を低コストで達成できること，すなわち要件 3) を満たすことを見出した．

そして [18] では，提案方式の主要処理をプロトタイプ実装し，地上実験で時刻のずれを計測し，同期がとれることを確認した．そして，実験結果を踏まえたセキュリティモデルを定め，提案方式の安全性を証明した．

これにより，地上実験までの 要件 1)〜3) の評価においては，情報理論的安全な暗号方式が最良の選択といえた．本稿では飛行環境下における要件 4) 実装の信頼性 (演算回路・ストレージの信頼性) を評価し，要件 1)〜4) の全ての評価項目において適切な暗号方式の選択を目指す．

3. 適切な暗号方式の選択に向けた検討

小型衛星・小型ロケット用通信システムは，前章の要件 1)〜4) を満たすべきである．

要件 1) の計算効率と回路規模の観点から，公開鍵系の暗号は対象外であり，情報理論的安全な暗号，軽量暗号，AES に代表される汎用用途ブロック暗号 (general-purpose block ciphers) が利用可能な候補として挙がる．

これらの一般的な位置付けは以下の通りである．

- 情報理論的安全な暗号は，要件 2) 高セキュリティと

[*1] 正式名称「宇宙品質にシフト MOMO3 号機」

表 1　情報理論的安全な暗号，軽量暗号，汎用用途ブロック暗号の要件 1)〜4) による評価結果.

評価項目	情報理論的安全な暗号	軽量暗号	汎用用途ブロック暗号
要件 1) 計算効率と回路規模	✓	✓	
要件 2) 高セキュリティ	✓		
要件 3) 低コスト	✓		✓
要件 4) 演算装置の信頼性	✓	–	要検証
要件 4) ストレージの信頼性	要検証	–	✓

✓: 要件を高いレベルで満たすことを表す．要検証: 飛行環境下における検証を要することを表す．–: 選択対象外のため未評価.

いう観点であれば最良だが，鍵サイズが大きい (ストレージコストが高い) という課題がある．

- 軽量暗号は，要件 1) 計算効率と回路規模，要件 3) 低コストについては最良だが，安全性に課題がある．
- 汎用用途ブロック暗号は要件 1)〜3) のいずれに関しても中間的な位置付けだが，演算回路の規模が他の二つに比べて大きいという課題がある．

ソフトウェア実装およびハードウェア実装における比較の結果は以下の通りである [20].

- 情報理論的安全な暗号における鍵サイズの課題は，ライフタイムが比較的短く総通信量が抑えられることより問題ない (低コスト汎用メモリに十分格納できる).
- 汎用用途ブロック暗号の回路規模については，情報理論的安全な暗号より大きいが，低コストのプラットフォームで実装可能なため問題ない．

よって，あえて安全性に課題のある軽量暗号を使う強い動機はなくなり，情報理論的安全な暗号と汎用用途ブロック暗号が利用可能な候補として残る．

次に改めて情報理論的安全な暗号と汎用用途ブロック暗号を比較する．ただし，要件 1) 計算効率と回路規模，要件 3) 低コストは問題が無いとして，残りの要件 2) 高セキュリティと要件 4) 実装の信頼性を検討する．

- 要件 2) 高セキュリティ
  情報理論的安全な暗号は計算リソースに制限のないあらゆる攻撃に対して安全性を保証する．一方，汎用用途ブロック暗号は，あくまでも現在知られている現実的な攻撃に対する安全性であり，時間経過や技術発展に伴い，新たな脆弱性が発見される可能性が否定できない [1]．よって，情報理論的安全な暗号の方が安全性が高い．
- 要件 4) 演算装置の信頼性
  情報理論的安全な暗号の方が回路規模が小さいため [20]，ソフトエラー (宇宙線に起因するデータ破損) やハードエラー (素子の恒久的な故障) による演算装置の信頼性低下リスクが低い．すなわち，情報理論的安全な暗号の演算装置の信頼性が高い．
- 要件 4) ストレージの信頼性
  汎用用途ブロック暗号の方が鍵サイズが小さいため，ソフトエラーやハードエラーによるストレージの信頼性の低下リスクが低い．すなわち，汎用用途ブロック暗号の方がストレージの信頼性が高い．

以上の評価結果を表 1 にまとめる．すなわち，ストレージの信頼性が実用上十分であれば，情報理論的安全な暗号が最良の選択と言える．

よって飛行実験においては，ストレージの信頼性を評価する．もしストレージの信頼性が実用上不十分であれば，汎用用途ブロック暗号も候補となるため，演算装置の信頼性も評価する．

4. 飛行実験

4.1 実験目的

本実験の目的は，提案方式が実際の飛行において正常に機能することの実証である．システム全体を統合した状態では問題の発生箇所や原因の特定が行いにくい．そこで今回，ソフトウェアやハードウェアの構成要素が個別に正しく動作するか確認することを主目的として，飛行実験を行った．特に，鍵ストレージに正常にアクセスできることの確認に重点をおいた．

4.2 実験内容

今回は，2019 年 5 月 4 日に打ち上げられた観測ロケット MOMO[24] の 3 号機に実験ハードウェアを搭載した（図 1）．このロケットは衛星軌道には到達せず，カルマン・ライン（一般に宇宙と呼ばれる高度 100km）を超える弾道飛行を行うものである．このため衛星と同様の放射線環境にはさらされない．しかし環境が厳しい宇宙ロケットの飛行初段部分において生じる以下の諸問題に関して，実環境評価を行うことが可能である．

- 距離: 地上局から 100km（MOMO）〜数千 km（軌道投入機）遠ざかっていくことにより，無線通信の BER 悪化や遅延増大が起こる可能性がある．
- 速度: 秒速 1km（MOMO）〜8km（軌道投入機）の高速度へ急加速していく過程で，無線通信においてドップラーシフト（周波数ずれ）等が継続的に発生し，受信障害が起こる可能性がある．
- 振動: エンジン燃焼，音響，空力などが原因となって振動が発生し，機器が共振を起こして破損することもある．また，オシレータの精度が悪化したり，機械的接点不良による誤動作（たとえばメモリカードのアクセス不良）が起こる可能性もある．

- 加速度: 機器に力が加わり破損する可能性がある．
- 温度: 電子機器は必ずしも宇宙空間に暴露されるとは限らないが，それでも地上での屋外利用と同様の温度にはさらされる．

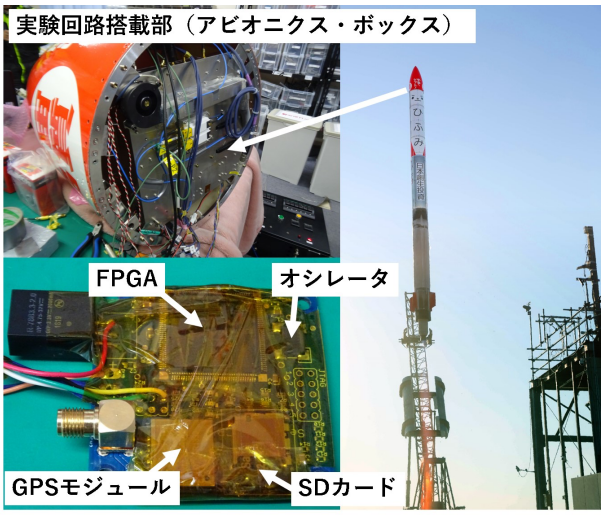

図 1　MOMO3 号機に搭載した実験用回路とその打ち上げ

以上の環境条件において [20] の提案方式が正しく機能するか調べるため，本実験では図 2 に示す構成の実験ハードウェアを用意した．動作を調べる構成部品とその選定理由は以下のとおりである．

- GPS(GNSS) 受信モジュール：Linx 社製の一般的なモジュール RXM-GPS-RM を用いた．大半の一般民生モジュールは利用可能な速度（600m/s）と高度（60000 フィート）に制限がある．MOMO を含め小型ロケットや小型衛星では，制限のない特殊なモジュール（[17] など）を用いる．しかし今回は，GPS モジュールの実証試験は MOMO の機体側でも行われることと，飛行途中で故障等により受信ができなくなった状況を模擬したいことから，本実験用には一般品を用いた．
- オシレータ：ABRACON 社製の民生 MEMS 製品を用いた．周波数安定性は ±10 ppm（1 分あたり最大 0.6 ミリ秒の誤差）と標準的水準である．MOMO における正確な振動環境が不明であったため，耐振動性に定評のある MEMS 製品を用いたが，GPS モジュールの補正が効かなくなった時の蓄積誤差が比較的大きいという欠点もある．
- SD カード：鍵ストレージとして，大容量，低価格，小型，低電力，交換容易性等の特徴を兼ね備えた民生マイクロ SD カード（Sandisk 社製 32GB Class 10）を用いた．
- FPGA：入手容易な民生品である Intel 社 MAX10 10M50SCE144I7G（動作保証温度範囲-40 ℃〜100 ℃）を用いた．

FPGA 内にはオシレータで直接駆動される時刻カウンタがあり，GPS 衛星が補足されている場合には，GPS モジュールから出力される 1 秒パルス（誤差は 0.1 マイクロ秒未満）によりオシレータ誤差が補正される．提案方式のもとでは，このカウンタ値は鍵ストレージのアクセス・アドレス導出に使われる．また，FPGA 内で SD カードのテスト回路が並列動作しており，先頭セクタから順にランダム値の読み書きを約 1.6Mbps で行い，書いた値が正しく読めるかをチェックし続ける．今回は SD カードを鍵ストレージとしては使わず，単独動作のチェックを行う．特に，コネクタ接点など機械的振動や衝撃に弱い部分に悪影響がないことを確認する．

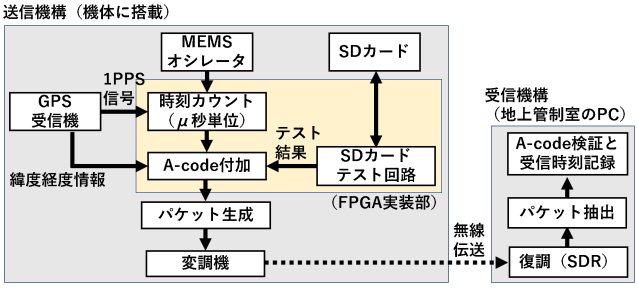

図 2　実験系のハードウェア構成

地上に伝送するパケット・ペイロードには，時刻カウンタ値，緯度・経度情報，SD カードのチェック結果，それらの A-code 値が含まれる（図 3）．A-code 計算は FPGA で行うが，FPGA が正常に演算を行っているかのチェックを容易にするため，鍵としては回路に埋め込みの固定値を用いた．

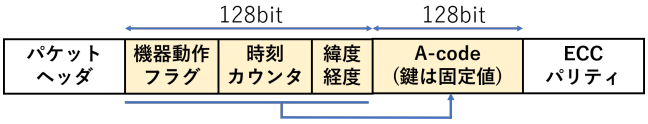

図 3　無線伝送するパケットのフォーマット

生成されたパケットは MOMO に搭載の無線送信器へ送られ，誤り訂正符号（2 シンボル訂正可能な弱いリードソロモン符号）のパリティ付加や π/4QPSK 変調などを行ったうえで，1 秒に約 3 回送信される（周波数帯は非公開）．すなわち，ロケット搭載の送信側ではほぼ全ての処理がハードウェアで行われ，処理時間の変動が少なく時刻精度も高い．いっぽう地上局では，復調，パケット抽出を経て A-code の検証を行い受信データが正しいかを調べるが，この一連の処理は SDR（Software Defined Radio）を含めたソフトウェアによって行い，計時は OS のシステム時計を用いた．このため，処理時間の測定結果には不確定要因があり，注意を要する．

4.3　実験結果

MOMO 3 号機の飛行の結果，打ち上げ前 20 秒から打ち上げ後 277.06 秒までの期間で本実験ハードウェアからの

データを取得できた．エンジン燃焼による加速は約 118 秒までであり，カルマンラインを超えたのは約 185 秒の時点である．GPS モジュール速度・高度制限を超えたのは約 83.7 秒の時点であり，少なくともその時点まではオシレータ誤差による時刻カウンタのずれはほとんどないと推定される．

上述の期間において，約 120 秒の時点で無線受信が少し途切れているものの（エンジン停止後に機体が回転し，アンテナの死角に入った事等が原因と考えられている），継続的に正常パケットを受信できた（図 4 の赤プロット）．全受信パケット数は 1223 個（くわえてパケットの消失が 262 個あったと推定されている），そのうち ECC パリティ値が正しくない異常パケットは 11 個であった．A-code 値が誤っているパケットは異常パケットのみに限られていたため，FPGA は正常に演算処理をしていたと判断できる．

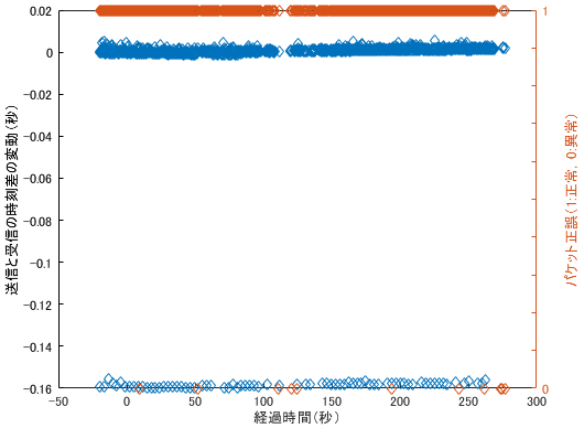

図 4　パケットの受信状況と遅延時間変動

また，SD カードについても，総計 348M ビット以上のアクセスを行ったことになるが異常は発見されなかった．フライト中に実験ハードウェアに加わった加速度は最大で約 5G，振動強度は 3grms 程度であり（おおよそ車程度），機械的な故障が発生する水準ではない．

以上より，本実験の主たる評価対象である鍵ストレージを含めたハードウェア信頼性については，今回とくに問題は発生しなかったと言える．

4.4　提案方式の改良につながる観察事項

ハードウェア信頼性とは別に，ロケットと地上局の通信遅延について，本提案方式の改良につながる事象が観察されたため説明する．改良の検討については **5.2** で改めて述べる．

図 4 の青プロットは，パケットに記されていた送信時点の GPS 時刻と地上での受信時刻（GPS ではなく PC で計時）の差分が，最初の点（打ち上げ 20 秒前）を基準としてどれだけ増減したかを表している．同図のように大半が 0 近辺にあるが，散発的に −0.16 秒近辺にも点がある．このうち後者は，ソフトウェアによる受信処理，とくに SDR 処理の時間ゆらぎが主原因であると推定される．ロケットと地上局は高々 100km ほどしか離れていないため電波の伝搬遅延増加は 0.3 ミリ秒程度しかなく，それだけでこれほど大きな変動にはならないと考えられるからである．

そこで遅延が 0 近辺にある点につき，時間スケールを拡大したのが図 5 の赤プロットである．打ち上げ直後は遅延がやや減少していき，80 秒ごろからは逆に平均遅延が 1.5 ミリ秒ほど増加する．打ち上げ前にロケットが地上にいる間は，このような変動は観察されていない（図 6）．このため，遅延変動は打ち上げ時に特有な現象である可能性が高い．

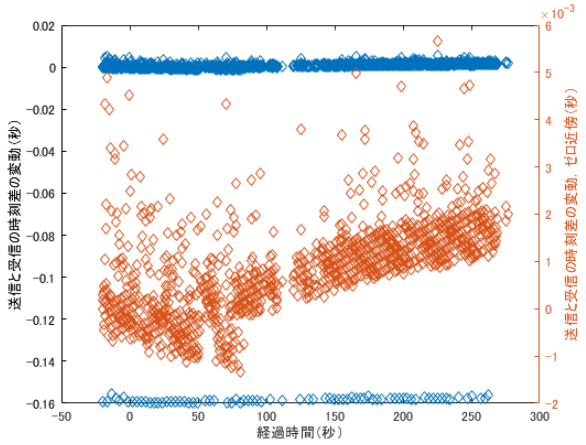

図 5　ソフトウェア受信処理時間の変動を除去した遅延時間

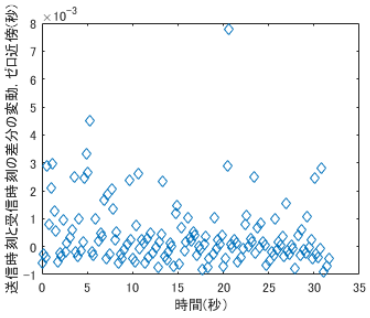

図 6　地上における遅延時間変動

遅延変動と機体の距離・速度を対比したのが図 7，図 8 である．速度と遅延時間の相関は低いが，距離についてはある程度の相関を見て取れる．原因については断定できないが，電波の伝搬時間の増加（約 0.3 ミリ秒）に加え，電波強度の減少により復調処理にかかる時間が増加した可能性や，オシレータ誤差により機上時刻カウンタがずれた可能性（打ち上げ後 83.7 秒前後から発生しうる）もある．

軌道投入用ロケットや衛星の場合，地上局との距離はより大きく変化するため，宇宙機と地上局との間の GPS（GNSS）時刻差も大きく（10 ミリ秒オーダで）変動するものと予想される．したがい，[20] で提案した各々が時刻情報から鍵を取得するアルゴリズムでは，鍵の同期に失敗する可能性が高まると思われる．

Vol.2019-CSEC-86 No.10
Vol.2019-SPT-34 No.10
2019/7/23

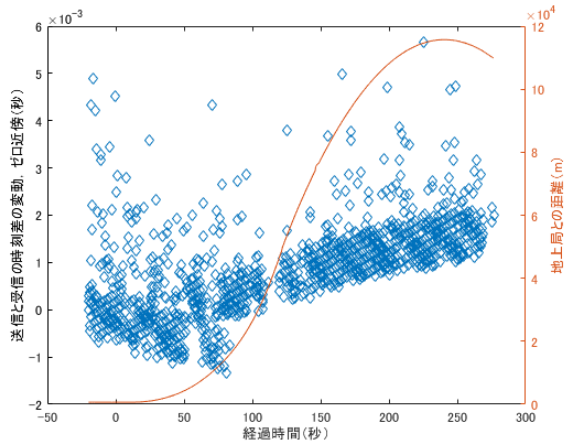

図 7　機体距離と遅延時間変動

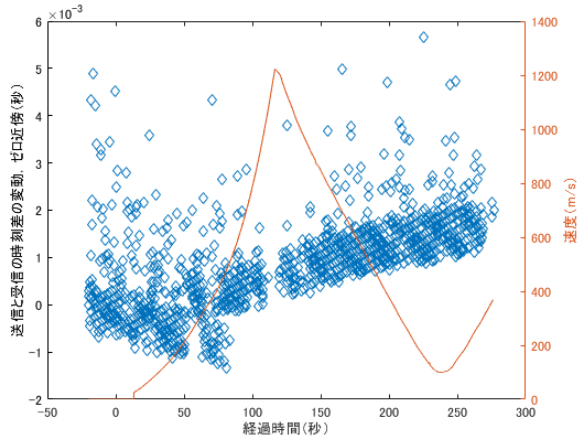

図 8　機体速度と遅延時間変動

4.5　その他の考察

液体燃料ロケットの初段として MOMO は典型的な飛行条件であり，他の液体燃料ロケットでも本実験装置は同様に動くと思われる．これに対し，固体燃料ロケットでは振動や加速度の条件が大幅に厳しくなるため，とくに SD カードのような機械的接点（コネクタ）を要するデバイスが利用できるかは懸念がもたれる．カードメモリでなく不揮発メモリチップを利用することが解決となり得る．

今回の観測ロケットでは半導体デバイスへの放射線の影響が試験できないが，必ずしも実フライトを実施しなくとも，地上の放射線照射施設で試験することは可能である．また，これまでに超小型衛星の飛行で民生半導体デバイスの宇宙利用について多くの知見が得られており，今回使っている FPGA やメモリも類似の民生品であるため，重大な懸念はそれほどないものと予想される．

5.　改良方式の提案と評価

本章では，[20] で著者らが提案した小型ロケットと地上局間のセキュア通信方式 (以下，宇科連方式と記す) を改良した方式とその安全性の評価結果を示す．なお，セキュリティモデルは [18] の定義に基づく．

5.1　改良の目的と方針

改良方式の目的は鍵の同期機構を変更することによる信頼性の向上にある．宇科連方式では，地上局と小型ロケットがそれぞれ測位衛星から時刻情報を取得し，各々が取得した時刻情報に基づき秘匿および認証を行うための鍵を決定していた．これに対して改良方式では，送信者 (アップリンクにおいては地上局，ダウンリンクにおいては小型ロケット) が，測位衛星から取得した時刻情報に基づいて鍵を決定し，決定した鍵を受信者が特定するための情報を送信データの一部に含めることで鍵の同期を実現する．宇科連方式では，地上局と小型ロケットが取得した時刻情報にずれが生じた場合，鍵の同期に失敗する課題が存在していたが，改良方式では送信者が使う鍵を指定することで鍵の同期に失敗するリスクがなくなり，信頼性が向上する．

用いる鍵を送信者が指定することにより，送受信者が過去に利用した鍵で受信データの認証を行うよう攻撃者がデータを偽造することが可能となる．このような攻撃を防ぐため，方式では，受信者は最後にデータを受信した際に利用した鍵の情報を記録し，認証対象のデータが指定する鍵が記録された鍵より後に用いるものであることを確認する対策を講じている．

5.2　改良方式

改良方式の詳細を記す．宇科連方式と同様，改良方式においても A-code をデータの認証に用いるだけでなく，通信時のデータと無通信時のランダムノイズの識別が困難な通信路から通信データを特定するためにも利用している点が特徴としてあげられる．

改良方式では，宇科連方式と同様アップリンクで飛行コマンド，ダウンリンクで飛行ステータス・データを送信するが，行う処理は両リンクで共通のため，方式の記述においては二つの通信路を区別せず，単に C と記す．

5.1 で述べた通り，改良方式では秘匿，および認証で用いる鍵の同期のために測位衛星から取得する時刻情報 (オラクル $\mathcal{O}_{\mathsf{GNS}}$ へのアクセスでモデル化) を利用する．具体的には，送信者は取得した時刻情報 t から鍵のインデックス idx を算出し，秘匿および認証に用いる鍵を決定するとともに，idx を通信路を通して受信者に送信する．この処理を実現するため，方式では送信者が時刻情報 $t \in \mathcal{T}$ からインデックスを算出する関数 $\mathsf{GetIdx} : \mathcal{T} \to \{0,1\}^T$ の存在を仮定する[*2]．

鍵生成: 全通信でやりとりされる総データ数 L，各データのビット長 ℓ，正当性に関するセキュリティパラメータ ϵ_{cor}，偽造不可能性に関するセキュリティパラメータ ϵ_{sec}，および絶対時刻からのゆらぎの上限値を表すジッタパラメータ jit_{GNS} を入力とし，L 個の A-code 鍵 $(k_{A,1}, \ldots, k_{A,L}) \in \mathcal{K}^L$，およ

[*2] GetIdx の具体的な実現法については本論文のスコープ外とする．

び L 個のワンタイムパッド鍵 $(k_{S,1},\ldots,k_{S,L}) \in \{0,1\}^{\ell \cdot L}$ を生成し，$k=(k_1,\ldots,k_L)$ $(k_i=(k_{S,i},k_{A,i}))$ を出力．生成された鍵は，地上局とロケットのストレージに格納される．ここで，用いる A-code $(\mathcal{K},\{0,1\}^{\ell+T},\{0,1\}^{\ell+T+n},A)$ は，L, およびデータ受信アルゴリズムのパラメータ MaxTrial に対して，$\min(\frac{\epsilon_{\mathsf{sec}}}{L\cdot \mathsf{MaxTrial}},\frac{\epsilon_{\mathsf{cor}}}{L\cdot \mathsf{MaxTrial}})$-偽造不可能性を有するものとする．

データ送信: 送信者は，平文 s の送信にあたり，オラクル $\mathcal{O}_{\mathsf{GNS}}$ から得られた時刻情報 t に基づいてインデックス $idx \leftarrow \mathsf{GetIdx}(t)$ を計算し，利用する鍵 k_{idx} を決定した後，Encrypt-then-MAC によって秘匿および認証処理を施して通信路 C にデータを出力する．具体的な処理は以下のようになる．

$\mathsf{Snd}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}(k,s)$
1. $t \leftarrow \mathcal{O}_{\mathsf{GNS}}$
2. $idx \leftarrow \mathsf{GetIdx}(t)$
3. $(k_S,k_A) \leftarrow k_{idx}$
4. $c \leftarrow s + k_S$ // ワンタイムパッドによる暗号化
5. $a \leftarrow A(k_A,(idx,c))$ // (idx,c) に対する認証子計算
6. **output** $((idx,c),a)$

データ受信: 暗号文の受信にあたり，受信者はノイズを含み，揺らぎのある通信路 C からを平文を抽出するために，C から暗号文長分のデータ $m=((idx,c),a)$ を暫定的に抽出し，復号に用いる鍵 $k_{idx}=(k_S,k_A)$ を決定する．次に，認証子生成関数 A を用いて $a=A(k_A,(idx,c))$ が成立するか否かを検証し，検証に成功した場合は $m=c-k_S$ により平文を復号する．検証に失敗した場合は，(c,a) を抽出する位置を 1 ビットずらし，上述の手順を繰り返しながら正しい平文を探索する (繰り返し回数を MaxTrial とする)．このようにして通信路から暗号文の抽出を行うことにより，高い確率で通信データのみを抽出することが可能となる．データ受信アルゴリズムの擬似コードは以下のように表される．なお，以下のコードにおいて o は，前回の Rcv 実行時に通信路から最後に切り出したデータの位置を記録する変数，$prev$ は最後に受信データを受理した際に用いた鍵のインデックスを記録する変数である．

$\mathsf{Rcv}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}(k)$
1. $o \leftarrow o+\ell+n$
2. $cnt \leftarrow 0$
3. **while** $(cnt < \mathsf{MaxTrial})$ **do**
4. $((idx,c),a) \leftarrow \mathsf{C}[o:o+\ell+n]$
5. **if** $(idx > prev)$
6. $(k_S,k_A) \leftarrow k_{idx}$
7. **if** $a = A(k_A,c)$
8. $prev \leftarrow idx$
9. **output** $c-k_S$
10. $o \leftarrow o+1$
11. $cnt \leftarrow cnt+1$
12. **output** $\perp$

Snd がデータを送信する頻度・タイミング，およびデータ通信に要する時間を考慮して Rcv を適切な頻度・タイミングで実行することにより，通信で生じる揺らぎに起因する通信路の同期ずれが MaxTrial ビット以下に収まる限り，方式の正当性は高確率で保証される．さらに，方式の安全性は通信で生じる揺らぎ，時刻の揺らぎに関わらず高確率で保証される．

定理 1 改良方式 $(\mathsf{Gen},\mathsf{Snd},\mathsf{Rcv})$ は ϵ_{cor}-正当性，ϵ_{sec}-偽造不可能性，および完全秘匿性を満たす．

証明: Snd アルゴリズムの入力となる平文 s はワンタイムパッドで暗号化されているため完全秘匿性は自明である．以下，方式の偽造不可能性，正当性について証明する．

はじめに ϵ_{sec}-偽造不可能性を示す．送信者が idx で示される鍵を用いて Snd アルゴリズムを実行した直後に敵が通信路を偽造する状況を考える．不正により偽造されたデータが $((idx',c'),a')$ 通信路から抽出されるが，この時以下の 3 種類のケースが考えられる．

ケース 1) $idx' \le prev$ が成立する場合: この場合は，受信アルゴリズムの 5 行目の処理により $((idx',c'),a')$ が受理される確率は 0 となる．

ケース 2) $prev < idx' \le idx$ が成立する場合: この場合に受信者が送信者が送っていない $((idx',c'),a')$ を受理する確率は A-code の改竄成功確率に一致するため $\frac{\epsilon_{\mathsf{sec}}}{L\cdot \mathsf{MaxTrial}}$ 以下となる．

ケース 3) $idx' > idx$ が成立する場合: この場合に受信者が $((idx',c'),a')$ を受理する確率は A-code の偽造成功確率に一致するため $\frac{\epsilon_{\mathsf{sec}}}{L\cdot \mathsf{MaxTrial}}$ 以下となる．

以上，ケース 1 から 3 の全ての場合に関して，Rcv が不正なデータを受理する確率は $\frac{\epsilon_{\mathsf{sec}}}{L\cdot \mathsf{MaxTrial}}$ 以下となる．地上局と小型ロケットの通信時に認証子の検証を行う回数は高々 $L\cdot \mathsf{MaxTrial}$ であるため，敵がデータの偽造，および改竄に成功する確率は高々 $(L\cdot \mathsf{MaxTrial})\cdot \frac{\epsilon_{\mathsf{sec}}}{L\cdot \mathsf{MaxTrial}} = \epsilon_{\mathsf{sec}}$ となり，ϵ_{sec}-偽造不可能性が示された．

次に正当性を示す．正当性が成立しない状況は，Rcv アルゴリズムが通信路から正当なメッセージを切り取る前に，$a' = A(k_{idx'},(idx',c))$ が成立するようなデータ $((idx',c'),a')$ が通信路から一度でも抽出された場合に起こる．このとき，$a' = A(k_{idx'},(idx',c))$ が成立する確率は idx' の値によって 3 種類のケースに分類されるが，いずれのケースにおいても偽造可能性の議論と同様にして，その確率が $\frac{\epsilon_{\mathsf{cor}}}{L\cdot \mathsf{MaxTrial}}$ 以下となることが示される．通信時に受信側が認証子の検証を行う回数は高々 $L\cdot \mathsf{MaxTrial}$ であるため，正当性が成立しない確率は高々 $(L\cdot \mathsf{MaxTrial})\cdot \frac{\epsilon_{\mathsf{cor}}}{L\cdot \mathsf{MaxTrial}} = \epsilon_{\mathsf{cor}}$ となり，ϵ_{cor}-正当性が示された．

文献 [2] では, 認証子生成関数 $A : GF(2^n)^2 \times GF(2^n)^N \rightarrow GF(2^n)$ として次式を用いることで $\frac{N}{2^n}$-偽造不可能性を満たす A-code が構成できることが示されている.

$$A((k_{A,0}, k_{A_1}), m) = k_{A,0} + \sum_{i=1}^{N} m_i \cdot k_{A,1}^{N-i+1}$$

改良方式では一度に $\ell + T$ ビットのデータを送信するため, 上述の A-code を利用する場合 $N = \frac{\ell+T}{n}$ となり, A-code は $\frac{\ell+T}{n2^n}$-偽造不可能性を有する. したがって, 任意の $\ell, T, L, \mathsf{MaxTrial}$ および ϵ に対して $\epsilon \leq \frac{(\ell+T)\cdot L\cdot \mathsf{MaxTrial}}{n\cdot 2^n}$ を満たすように n を選ぶことにより ϵ-正当性 ϵ-偽造不可能性, および 完全秘匿性を満たす方式 $(\mathsf{Gen}, \mathsf{Snd}, \mathsf{Rcv})$ を構成することが可能となる.

すなわち改良方式は, 任意に選択した ϵ に対して n を上式を満たすように選択することにより偽造が確率 $1-\epsilon$ でしか成功しないことを保証する. しかし攻撃者が確率 ϵ で一度でもメッセージの偽造に成功した場合は, 以後, 送信者が送ったメッセージが受理されなくなる課題が存在する. これは, 攻撃者が偽造したメッセージにより, Rcv アルゴリズムの変数 $prev$ の値が遠い未来の値に書き換えられ, その後の送信者が送ったメッセージが Rcv アルゴリズムの 5 行目の処理によって拒否されてしまうためである. この問題を解決するには, Rcv も時刻情報を取得し, メッセージ中の idx の値が, 取得した時刻情報と大きくずれていないことを確認する等の手段が考えられるが, 詳細な設計は今後の課題である.

6. おわりに

本稿では, 観測ロケット MOMO3 による実験を通じて, 著者らが提案するセキュリティ機構が実際の飛行環境下で正常に機能することを確認した. 今回の実験では, ストレージに保存した鍵に関しての破壊や演算回路の故障は発生せず, 小型ロケットの飛行環境での本方式の利用可能性に関して肯定的な結果が得られたと考えている. 今後の課題としては, 小型衛星への適用も視野に入れた信頼性検証や, 装置故障や攻撃への耐性向上と実装の検討などがあげられる.

参考文献

[1] A. Bogdanov, D. Khovratovich, and C. Rechberger, "Biclique Cryptanalysis of the Full AES," ASIACRYPT 2011, LNCS 7073, pp.344–371, Dec. 2011.
[2] B. den Boer, A Simple and Key-Economical Unconditional Authentication Scheme, Journal of Computer Security, Vol. 2, pp. 65–71, 1993.
[3] R. Canetti and M. Fischlin, "Universally Composable Commitments," Crypto 2001, LNCS 2139, pp.19–40.
[4] R. Cramer, R. Gennaro, and B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme," Eurocrypt '97, LNCS1233, pp.103–118, 1997.
[5] I. Damgård, "Efficient Concurrent Zero-Knowledge in the Auxiliary String Model," Eurocrypt 00, LNCS, 2000.
[6] A. Kuldmaa, "On Secure Bulletin Boards for E-Voting," Master's thesis, University of Tartu, 2017.
[7] V.Fischer and P.Haddad, Random Number Generators for Cryptography, Chapter 7, Circuits and Systems for Security and Privacy, CRC Press, 2016.
[8] M. Fischlin and R. Fischlin, "Efficient Non-Malleable Commitment Schemes," CRYPTO 00, LNCS1880, 2000, pp.413–428.
[9] R. Kanai and T. Inagawa, Development and Operation of a Hydrocarbon Liquid Propellant Orbital/Sub-Orbital Launcher, IAC-17.D2.7.10, 68th Intl. Astronautical Congress (IAC), Sep. 2017.
[10] H. Saito et al., World Fastest Communication from a 50kg Class Satellite, IEICE Communications Society GLOBAL NEWSLETTER, Vol.39, No.2, pp.3–7, 2015.
[11] C. E. Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal, vol.28-4, pp.656–715, Oct. 1949.
[12] G.J.Simmons, Authentication Theory / Coding Theory, Proceedings of CRYPTO 1984, LNCS, Vol. 196, Springer Verlag, pp. 411–431, 1984
[13] H. Takenaka et al., Satellite-to-Ground Quantum-Limited Communication Using a 50-kg-Class Micro-Satellite, 10.1038/nphoton.2017.107, Nature Photonics, 2017.
[14] G.S.Vernam, Cipher Printing Telegraph Systems for Secret Wire and Radion Telegraphic Communications, Journal of American Institute of Electrical Engineers, 45, pp.295–301, 1926.
[15] 阿部まみ他: 次世代衛星向けミッションデータ処理装置の開発, 第 57 回宇宙科学技術連合講演会, 1H04, 2013.
[16] 上野, 森岡, 本間: 情報理論的に安全な鍵長可変 MAC ハードウェアアーキテクチャの設計. 2019 年暗号と情報セキュリティシンポジウム (SCIS2019), 1D1-3, 2019.
[17] 海老沼拓史: 衛星搭載用小型 GNSS スマートアンテナの開発, 第 61 回宇宙科学技術連合講演会, 3B06, 2017.
[18] 尾花, 吉田, 森岡: 小型衛星・小型ロケット用通信のセキュリティモデルとプロトタイプ実装. 情報処理学会研究報告, Vol.2019-CSEC-84, No.3, 2019.
[19] 四方順司, 渡邊洋平: 情報理論的暗号技術について, 情報処理学会学会誌, Vol.55 No.3, pp. 260–267, 2014.
[20] 森岡, 尾花, 吉田: 超小型衛星・小型ロケット用セ キュア通信のための情報理論的安全性の検討. 第 62 回宇宙科学技術連合講演会. 1K19, 2018.
[21] 内閣府宇宙開発戦略推進事務局: 人工衛星等の打上げ用ロケットの型式認定に関するガイドライン改訂第 1 版, 平成 30 年 3 月 30 日, http://www8.cao.go.jp/space/application/space_activity/documents/guideline2.pdf
[22] 内閣府宇宙開発戦略推進事務局: 人工衛星等の打上げに係る許可に関するガイドライン改訂第 1 版, 平成 30 年 3 月 30 日, http://www8.cao.go.jp/space/application/space_activity/documents/guideline1.pdf
[23] 内閣府宇宙政策委員会: 小型・小型衛星の打ち上げ需要調査概略版, 宇宙産業・科学技術基盤部会第 39 回会合資料 5, 平成 30 年 5 月 28 日, http://www8.cao.go.jp/space/comittee/27-kiban/kiban-dai39/gijisidai.html
[24] User's guide of sounding rocket MOMO, http://www.istellartech.com/7hbym/wp-content/themes/ist/img/technology/MOMOUsersguidever.0.2.pdf