Vol.2019-DPS-178 No.3
Vol.2019-CSEC-84 No.3
2019/3/4

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

尾花 賢[1]　吉田 真紀[2]　森岡 澄夫[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．同法律はロケット打ち上げや管理に関する許可制度を含んでおり，民間事業者が宇宙ビジネスに参入する新たな宇宙時代の幕開けを示唆している．同法律の関連ガイドラインにはロケットの打ち上げに際して「重要なシステム等に関する信号の送受信については，妨害や乗っ取りの被害にあわないよう，適切な暗号化等の措置を講ずること」との記述があり，衛星やロケットの打ち上げに際しては通信セキュリティの確保が必要である旨明記されている．しかしこの記述は抽象度が高く，地上局とロケット・衛星の間にどの程度のセキュリティが必要か具体的には定義されていない．本稿はこのような状況に鑑み，近年日本が国際競争力強化を目指している小型衛星・小型ロケットに対しセキュリティモデルを提案する．また，提案したセキュリティモデルの下で，著者らが提案している方式の安全性を示すとともに，無線機器，GNSS 受信機，および FPGA を用いてプロトタイプ実装を行い，地上での実験を通して動作することを確認した．

キーワード：小型衛星，小型ロケット，無線通信，セキュリティモデル，プロトタイプ実装

A Security Model and a Prototype Implementation of Communication System for Small Satellites and Small Launch Vehicles

1. はじめに

近年，(超) 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 [1]．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 [2]，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 [3], [4]．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．

それを受け，著者らは文献 [16] において，小型衛星や小型ロケットの通信において達成すべきセキュリティ要件を整理するとともに，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通信総量を分析し，現在衛星やロケットに搭載可能な計算リソースやメモリ・リソースの範囲で情報理論的安全性が実現できることを示した．さらに，ワンタイムパッド暗号 (通信目的によるが鍵の総量は数十 MB〜数 TB 程度) とガロア体上の多項式評価に基づく情報理論的に安全なメッセージ認証コード (A-code) を組み合わせた単純な方式を提案している．

既存の枯れた技術の組み合わせにより，小型ロケット・小型衛星用通信の実現に一定の目処が立ったため，次のステップとして，小型ロケット・小型衛星用通信に関するフォーマルなセキュリティモデルを提案することが考えられる．それにより，提案した暗号プリミティブの組み合わせに限らず，秘匿機能付き認証コードや情報理論的に安全

[1] 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
[2] 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
[3] 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

な認証暗号 (Authenticated Encryption) などの最新の成果を取り入れた方式の安全性を数学的に評価することが可能となる．

そこで本稿ではまず文献 [16] で整理したセキュリティ要件に基づき，小型ロケット・小型衛星用通信に関するフォーマルなセキュリティモデルを提案する．次に，提案したセキュリティモデルの下で，文献 [16] で提案した方式の安全性評価を行った．そして，通信方式のプロトタイプとして，FPGA，無線通信機器，GNSS (Global Navigation Satellite System) の受信機を組み合わせた本番環境に近いシステムを実装し地上実験を行うことでその有効性を確認した．具体的には，小型ロケットと地上局間の通信を想定した無線伝送実験を行い，GNSS を用いた鍵の同期機構やメッセージ認証コードによる送信データの非改竄性の検証が有効に機能することを確認した．

本稿の構成は以下の通りである．2. では文献 [16] で行った対象とする通信システムの分析，およびその結果として得られた定性的なセキュリティ要件を概説する． 3. では，2. の定性的要件を踏まえたフォーマルなセキュリティモデルを提案する．4. では文献 [16] で提案した方式の説明，および 3. で定義したセキュリティモデルの下での方式の安全性について述べる．5. では 4. に示した方式のプロトタイプを実装し，無線通信を用いて地上実験を行った結果を示す．最後に 6. でまとめと今後の検討課題を述べる．

2. 小型衛星・ロケット用通信の概要

著者らが文献 [16] で分析および整理した，小型衛星・ロケット用通信システムの構成，想定される攻撃，セキュリティ要件の要旨を示す．

2.1 対象システムにおけるエンティティ

通信システムにおける信号の送受信は，以下のエンティティ間で行われるものとする．

2.1.1 地上局 (GS, Ground Station)

小型衛星や小型ロケットの管制を無線交信により行う．複数の局が設置される場合もあるが，一時点では一局のみが交信を行う．各局には無線送受信機やアンテナ，電源装置などが設置され，外部からの支援なく単独で機能維持できる．無線処理系は局外との通信系からは分離されている．

2.1.2 小型ロケット (SLV, Small LaunchVehicle)

小型衛星を地球低軌道 (LEO) に打ち上げる．地上局との無線通信に対し，安全上の観点から可用性への強い要求がある．すなわち，緊急時には地上局から中断コマンドが (繰り返し) 送られ，予め定められた短時間内 (多くは数秒以内) に確実に実行されなければならないという要求がある．ダウンリンクについても可用性が求められており，地上局における飛行状況把握が低遅延・高頻度 (数 Hz〜100Hz 程度) でできねばならない．小型ロケットのライフタイムは短く，無線交信も打ち上げ前数時間から打ち上げ後数十分 (衛星分離まで) しか行われない．データレートは 10Kbps〜10Mbps 程度である．機上の計算リソースとしては，重量・電力の制限はあるものの，組み込み向け CPU や FPGA が利用可能である．

2.1.3 小型衛星 (SS, Small Satellite)

LEO を数か月〜数年に渡って周回し，学術・商用ミッションを遂行する．小型ロケットと比べ制御に関わる通信は少ないが，ダウンリンクのミッションデータも保護すべき対象となる．ミッションデータの量は増加傾向にある．ダウンリンク速度は従来 100Kbps〜数十 Mbps が上限であったが，今後は光通信導入も行われ数百 Mbps〜数 Gbps に達する見込みである [9], [10]．機上の計算リソースとして，FPGA や動作クロック 1GHz クラスのプロセッサなども利用可能となっている．民生電子デバイスの耐放射線性は著しく向上しているが，中長期の運用中にはソフトエラーやハードエラーの影響が蓄積・顕在化しうる．

2.1.4 測位衛星 (GNS, GNSS Satellite)

受信者が位置と時刻情報を算出できるようにするための情報を送信する．地上局と小型ロケットは GNSS 受信機を備える．小型衛星では GNSS 受信機は必ずしも搭載されない．

以降では，小型ロケット・小型衛星を，単にロケット・衛星と呼ぶ．

2.2 対象システムにおける通信

エンティティ間の無線通信を対象とする．現状の運用では無線通信は地上局と小型ロケット，地上局と小型衛星の間で行われ，小型ロケットと小型衛星との間および地上局間に無線通信はない．

信号の送信時に，送信者は信号の元となるデータの種類に応じて予め定められた長さに分割し，各種処理を施して送信する (以降，処理が施される前のデータを平文と呼ぶ)．無通信時には受信者はノイズを受けとる．

無線通信に要する時間には揺らぎが生じるが．その上限値は予め分かっているものとする．

2.3 無線通信で想定される攻撃

想定される攻撃は，信号の送受信に対する人的攻撃と環境的攻撃に大別できる．なお，以降では地上局と小型ロケットおよび地上局と小型衛星の通信について議論する．他のエンティティ間の通信も同様に議論できるため，ここでは言及しない．

2.3.1 人的攻撃

信号の送受信における攻撃の主体 (攻撃者と呼ぶ) は以下の高い能力を有するが，エンティティに物理的にアクセスすることはできないとする．

受動的 (盗聴・推測)　地上局・ロケット・衛星が発する無線電波の周波数を検知し，傍受や信号波形の記録ができる．さらに，平文データが伝送されている場合には，その

信号波形から変調方式やデータ内容を推定できる．これにより，管制情報の解析や，高価値ミッションデータの盗聴が可能となる．

能動的 (なりすまし・改ざん)　記録どおりの信号や推定に基づいて改ざんした信号を十分な強度で送信できる．その結果，管制情報・ミッションデータの改ざんやエンティティのなりすましが可能となり，飛行中断・継続コントロールを含むミッション遂行ができなくなる．

破壊的 (妨害)　ノイズ信号などを十分な強度で送信できる．これは，通信障害を引き起こし，飛行中断・継続コントロールを含むミッション遂行ができなくなる．

2.3.2 環境的攻撃

宇宙空間でハードウェア機器を利用することによって，データやハードウェアの一時的ないし恒久的な損失・損傷・不正動作等の影響がある．

本稿で提案するモデルは，人的攻撃のうち，受動的・能動的攻撃のみを対象とし，測位衛星からの信号の受信妨害を含む破壊的攻撃への対策は今後の課題とする．

2.4 望まれるセキュリティ

人的攻撃や環境的攻撃のもと，セキュリティとして以下の三つを満たすことが望まれる．なお，狭義のセキュリティは秘匿と認証の二つだが，近年，可用性もセキュリティ要件として議論されることがある．

2.4.1 秘匿

アップリンクにおいて，地上局が作成した情報は，当該地上局が意図したロケット・衛星のみが入手できる．ダウンリンクも同様.

2.4.2 認証

地上局が作成した情報は，ロケット・衛星側において，作成者が当該地上局であり，他者による改ざんがないことを確認できる．ダウンリンクも同様.

2.4.3 可用性

予め定められた期間に地上局が送出した情報を，予め定められた時間内にロケット・衛星は入手できる．ダウンリンクも同様.

3. セキュリティモデル

本節ではロケット・衛星用通信システムのモデルを提案する．具体的には，通信に要する時間に揺らぎのある無線通信と，そこで送受信される信号に対する秘匿，認証，可用性を定義する．

3.1 アルゴリズム

個々のアルゴリズムの説明に先立ち，測位衛星からの時刻情報の算出と，二者間の無線通信の扱いを定義する．

3.1.1 測位衛星のモデル

測位衛星からの情報を受信し，時刻情報を算出できることをオラクルへのアクセスとしてモデル化する．オラクル $\mathcal{O}_{\mathsf{GNS}}$ にアクセスすると絶対時刻に対して揺らぎが加味された時刻が得られる．揺らぎの上限値を jit_{GNS} と定義する．

3.1.2 二者間の無線通信のモデル

二者間の無線通信をグローバルテープへの読み書きとしてモデル化する．グローバルテープは半無限のセルからなる．グローバルテープ C の第 i セルから第 $j-1$ セルまでの記号列を $\mathsf{C}[i:j]$ と記す．グローバルテープには地上局からロケットへのアップリンク $\mathsf{C}_U^{\mathsf{GS,SLV}}$，ロケットから地上局へのダウンリンク $\mathsf{C}_D^{\mathsf{SLV,GS}}$，地上局から小型衛星へのアップリンク $\mathsf{C}_U^{\mathsf{GS},SS}$，小型衛星から地上局へのダウンリンク $\mathsf{C}_U^{SS,\mathsf{GS}}$ の 4 種類が存在する．

以降，オラクル $\mathcal{O}$ にアクセスし，グローバルテープ C の読み書きを行うアルゴリズム Alg を $\mathsf{Alg}_{\mathsf{C}}^{\mathcal{O}}$ と記す．

提案モデルは，鍵生成アルゴリズム Gen，データ送信アルゴリズム $\mathsf{Snd}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}$，データ受信アルゴリズム $\mathsf{Rcv}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}$ の三種類のアルゴリズムから構成される．

$\mathsf{Snd}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}$ は C のビットレートに相当する速度で一方向に動くヘッドで備える．そして入力された鍵と平文から暗号文 $\{0,1\}^*$ を生成し，テープ C に書き込む．無通信時にはランダムな系列 $\{0,1,\perp\}^*$ を書き込む．ここで $\perp$ は信号が弱く 0 か 1 かを識別できないデータを表す．$\mathsf{Rcv}_{\mathsf{C}}$ は C のビットレートに相当する速度で一方向に動くヘッドで備える．そして入力された鍵と暗号文をテープ C から読み込み，暗号文の非改竄性チェックと暗号文の復号を行う．

以後，鍵の集合，平文の集合，暗号文の集合を表す記号として，それぞれ $\mathcal{K},\mathcal{S},\mathcal{M}$ を用いることとする

3.1.3 鍵生成アルゴリズム Gen

地上局，ロケット・衛星間でミッションの開始から終了までにやりとりされる総平文数 L，各平文のビット長 ℓ，正当性要件に関するセキュリティパラメータ ϵ_{cor}，安全性に関するセキュリティパラメータ ϵ_{sec} およびジッタパラメータ jit_{GNS} を入力として，地上局，ロケット・衛星が共有する共有鍵 $k \in \mathcal{K}$ を出力する．

3.1.4 データ送信アルゴリズム $\mathsf{Snd}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}$

共有鍵 $k \in \mathcal{K}$，および固定長の平文 $s \in \mathcal{S}$，およびインデックス idx を入力として，通信路を通して送る暗号文 $m \in \mathcal{M}$ を出力するとともにデータはヘッドを介して C テープに書き込まれる．

3.1.5 データ受信アルゴリズム $\mathsf{Rcv}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}$

共有鍵 $k \in \mathcal{K}$，およびインデックス idx を入力として，グローバルテープ C にアクセスすることで送信データの複号結果 $s' \in \mathcal{S}$ または $\perp$ を出力する．Rcv も Snd 同様測位衛星へのオラクルアクセス $\mathcal{O}_{\mathsf{GNS}}$ が可能である．

3.2 正当性

提案モデルにおける正当性は，可用性に対応し，送信者が送信したデータは高い確率で受信者に受信されることを要求している．より厳密には，モデルの正当性は以下のように定義される．

定義 1 $(\mathsf{Gen}, \mathsf{Snd}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}, \mathsf{Rcv}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}})$ が以下の式を満たすとき，$(\mathsf{Gen}, \mathsf{Snd}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}, \mathsf{Rcv}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}})$ は ϵ-**正当**であるという．

$$\Pr\left[\begin{array}{l} k \leftarrow \mathsf{Gen}(L, \ell, \epsilon_{\mathsf{cor}}, \epsilon_{\mathsf{sec}}, jit_{\mathsf{GNS}}); \\ \quad m \leftarrow \mathsf{Snd}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}(k, s, idx) \end{array} : \mathsf{Rcv}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}(k, idx) = s\right] \geq 1 - \epsilon$$

3.3 安全性

提案モデルにおける安全性は，秘匿と認証に対応する．認証に対する攻撃者はグローバルテープの読み書きが可能であり，適応的選択メッセージ攻撃の下，通信データの偽造を目的とする攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ の不正は以下のゲームによって記述できる[*1]．

$\mathsf{exp}(\mathcal{A}^{\mathsf{Gen},\mathsf{Snd},\mathsf{Rcv}}, \mathsf{C}, \mathcal{O}_{\mathsf{GNS}})$
1. $k \leftarrow \mathsf{Gen}(L, \ell, \epsilon_{\mathsf{cor}}, \epsilon_{\mathsf{sec}}, jit_{\mathsf{GNS}})$
2. $\mathsf{List}_{\mathsf{Snd}} \leftarrow \emptyset$
3. **for** $i = 1$ **to** L **do**
4. $\quad (s, \mathsf{state}) \leftarrow \mathcal{A}_1{}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}(\mathsf{state})$
5. $\quad m \leftarrow \mathsf{Snd}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}(k, s, i)$
6. $\quad \mathsf{List}_{\mathsf{Snd}} \leftarrow \mathsf{List}_{\mathsf{Snd}} \cup \{(s, i)\}$
7. $\mathcal{A}_2{}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}(\mathsf{state})$
8. **for** $i = 1$ **to** L **do**
9. $\quad s \leftarrow \mathsf{Rcv}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}(k, i)$
10. $\quad$ **if** $s \neq \perp$ **and** $(s, i) \notin \mathsf{List}_{\mathsf{Snd}}$ **then return** 1
11. **return** 0

定義 2 $(\mathsf{Gen}, \mathsf{Snd}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}, \mathsf{Rcv}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}})$ が任意の攻撃者 $\mathcal{A}$ に対して次式を満たすとき，ϵ-偽造不可能と定義する．

$$\Pr[\mathsf{exp}(\mathcal{A}^{\mathsf{Gen},\mathsf{Snd},\mathsf{Rcv}}) = 1] \leq \epsilon$$

提案モデルにおける秘匿は，Shannon による完全秘匿の概念に基づき次のように定義できる．

定義 3 S_i $(i = 1, \ldots, L)$ を i 番目に送信した平文の確率変数，M_i $(i = 1, \ldots, L)$ を i 番目の暗号文の確率変数とする．$(\mathsf{Gen}, \mathsf{Snd}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}, \mathsf{Rcv}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}})$ が任意の暗号文 $m_i \in \mathcal{M}$ と任意の $s_i \in \mathcal{S}$ $(i = 1, \ldots, L)$ に対して次式を満たすとき，$(\mathsf{Gen}, \mathsf{Snd}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}, \mathsf{Rcv}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}})$ は **完全秘匿**と定義する (ただし，次式の確率は鍵 k を鍵集合 $\mathcal{K}$ 上で確率分布にしたがって振ることによって計算する)．

$$\Pr[S_i = s_i, \ldots, S_L = s_L | M_1 = m_1, \ldots, M_L = m_L] = \Pr[S_i = s_i, \ldots, S_L = s_L]$$

[*1] 実環境の攻撃者は送信者が暗号化する平文をコントロールすることはできないが，本稿では適応的選択メッセージ攻撃を行う強力な攻撃者の下での安全性を考えることとする．

4. 著者らの提案方式 [16] の安全性評価

本節では，文献 [16] で著者らが提案した方式を説明するとともに，前節に提案したモデルの下での方式の安全性評価結果を示す．

文献 [16] で提案した方式の基本的なアイデアは，ワンタイムパッド [6] と認証コード (A-code)[7] を組み合わせることにより，秘匿機能付き認証コードを構成し，秘匿と認証を実現することである．方式の特徴的な点は，正当性を満たすために，認証コード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する点にある．

文献 [16] では，ロケット用の通信，衛星用の通信それぞれに適した二種類の方式を提案しているが，特にロケットの通信については，地上局との間のインタラクションを可能な限り排除する．これは，通信プロトコル上のエラー発生と，それに伴う制御喪失を回避するためである．

4.1 秘匿機能付き認証コード

ここでは，文献 [16] における提案方式のベースとなる情報理論的に安全な秘匿機能付き認証コード [15] (Unconditionally Secure Authentication Codes with Secrecy，以下 秘匿機能付き認証コードと記す) のモデルを概説する．秘匿機能付き認証コードは無制限の計算リソースを有する攻撃者に対して安全な秘匿と認証を実現する暗号技術であり，以下の五つ組 $(\mathcal{S}, \mathcal{M}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ によって定義される．

$\mathcal{S}$ ：平文 (source state) の集合
$\mathcal{M}$：通信路を通して送られる暗号文の集合
$\mathcal{K}$ ：送受信者間で共有される鍵の集合
$\mathcal{E}$ ：認証機能付き暗号化関数 $(\mathcal{E} : \mathcal{K} \times \mathcal{S} \rightarrow \mathcal{M})$ の集合
$\mathcal{D}$ ：認証機能付き復号関数 $(\mathcal{D} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{S} \cup \{\perp\})$ の集合

$\mathcal{E}$ および $\mathcal{D}$ の元は鍵 $k \in \mathcal{K}$ をインデックスとして一意に指定することができる．以降，鍵 k によって指定される $\mathcal{E}$ および $\mathcal{D}$ の元をそれぞれ E_k, D_k と記すこととする．

S, K をそれぞれ $\mathcal{S}, \mathcal{K}$ 上の確率変数としたとき，秘匿機能付き認証コード $(\mathcal{S}, \mathcal{M}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ は以下の正当性条件を満足する．

$$\Pr[k \leftarrow K; s \leftarrow S; m \leftarrow E_k(s) : s = D_k(m)] = 1$$

秘匿機能付き認証コードの認証を破ろうとする攻撃者 $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ の不正は以下のゲームによって定義される[*2]．ただし，以下において AE オラクル $\mathcal{O}_{AE}$ は，送受信者の共有鍵 $k \in \mathcal{K}$ を用いて平文の確率分布にしたがって選ばれた $s \in \mathcal{S}$ を暗号化した暗号文 $m = E_k(s)$ を出力するオラクルであり，E オラクル $\mathcal{O}_E$ は，$s \in \mathcal{S}$ を入力として，送受信者の共有鍵 $k \in \mathcal{K}$ を用いた暗号文 $m = E_k(s)$

[*2] 秘匿機能付き認証コードにおいて，より強力な攻撃者を想定するようなモデルも存在する．

を出力するオラクルである．

$\mathsf{exp}(\mathcal{A}^{(\mathcal{S},\mathcal{M},\mathcal{K},\mathcal{E},\mathcal{D})})$:
1. $\mathsf{state} \leftarrow \mathcal{A}_1^{\mathcal{O}_{AE},\mathcal{O}_E}(\mathcal{S},\mathcal{M},\mathcal{K},\mathcal{E},\mathcal{D})$
2. $m' \leftarrow \mathcal{A}_2(\mathsf{state})$
3. **if** $m' \notin \hat{\mathcal{M}}$ **and** $D_k(m') \neq \perp$ **return** 1
4. **else return** 0

定義 4　オラクルへのアクセス回数が L に限定された任意の攻撃者 $\mathcal{A}$ に対して，$m' \notin \hat{\mathcal{M}}$ かつ $D_k(m') \neq \perp$ となる確率が ϵ 以下となるとき，秘匿機能付き $(\mathcal{S},\mathcal{M},\mathcal{K},\mathcal{E},\mathcal{D})$ を (L,ϵ) **偽造不可能**と定義する．ただし，$\hat{\mathcal{M}}$ はオラクルが出力した暗号文集合である．

次に秘匿機能付きの完全秘匿性を以下のように定義する．

定義 5　秘匿機能付き $(\mathcal{S},\mathcal{M},\mathcal{K},\mathcal{E},\mathcal{D})$ が任意の暗号文 $m \in \mathcal{M}$ と任意の $s \in \mathcal{S}$ に対して次式を満たすとき，$(\mathcal{S},\mathcal{M},\mathcal{K},\mathcal{E},\mathcal{D})$ は**完全秘匿**と定義する (ただし，次式の確率は鍵 k を鍵集合 $\mathcal{K}$ 上で確率分布にしたがって振ることによって計算する)．

$$\Pr[S = s | M = m] = \Pr[S = s]$$

4.2　秘匿機能付き認証コードの構成法 [16]

ここでは，文献 [16] における提案方式のベースとなる秘匿機能付き認証コードの構成法について説明する．ベースとして用いる秘匿機能付き認証コードは，ワンタイムパッドと，既知 A-code を Encrypt-then-Mac により組み合わせたものである．具体的には，ワンタイムパッドの鍵 k_S と A-code の鍵 k_A を独立に用意し，平文 s をワンタイムパッドで暗号化した暗号文 $c = s + k_S$ と，暗号文 c に対する A-code の $a = A(k_A, c)$ のペア (c, a) を暗号文とするものである．

文献 [16] では，認証子の生成および検証に，次式で定義される関数 $A : GF(2^n)^2 \times GF(2^n)^\ell \to GF(2^n)$ を用いることで，完全秘匿かつ $(1, \ell/2^n)$-偽造不可能な秘匿機能付き認証コードを構成している．

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

4.3　小型ロケット用セキュア通信方式 [16]

本節では，文献 [16] で著者らが提案した地上局と小型ロケットの通信に適したセキュア通信方式を説明するとともに，提案モデルの下での安全性評価結果を示す．この方式では前述の秘匿機能付き認証コードを用い，提案方式ではアップリンク C_U で飛行コマンド，ダウンリンク C_D で飛行ステータス・データを送信するが，行う処理は $\mathsf{C}_U, \mathsf{C}_D$ 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 と記すこととする．

この方式では，ベースとなる秘匿機能付き認証コードを利用するため，ロケットと地上局で同じ鍵を用いるための同期機構が必須になる．この方式では地上局とロケットの両方に GNSS 受信機を設置し，取得した時刻情報から鍵のインデックスを算出することで鍵の同期をとる．具体的には送信者が取得した時刻 t_S からインデックスを算出する関数 GetIdx_S，および受信者が取得した時刻 t_R からインデックスを算出する関数 GetIdx_R を定義し，双方で同一のインデックスを算出する (つまり $\mathsf{GetIdx}_S(t_S) = \mathsf{GetIdx}_R(t_R)$ が成立する) 機構の存在を仮定する[*3]．

なお，以下の記述において平文長，暗号文長，単一の平文の暗号化・暗号文の復号に必要な鍵のビット長はそれぞれ $n, \ell+n, \ell+2n$ とする．また文脈から明らかな場合は，特に断りなしに n ビットのデータを $GF(2^n)$ の元と，ℓ ビットのデータを $GF(2^n)$ 上の ℓ' 次元ベクトルと同一視する (ただし $\ell' = \ell/n$)．具体的な方式は以下の通りである．

4.3.1　鍵生成

全通信でやりとりされる総平文数 L，各平文のビット長 ℓ，セキュリティパラメータ ϵ_{cor}，ϵ_{sec} およびジッタパラメータ jit_{GNS} を入力とし，$(\ell+2n)L$ ビットの乱数 $k = (k_1, \ldots, k_L)$ を出力する．ここで n は，L, ℓ, および jit_{GNS} から算出されるパラメータ $\mathsf{MaxTrial}$ に対して $\frac{\ell \cdot \mathsf{MaxTrial}}{n2^n} \leq \epsilon_{\mathsf{cor}}$，および $\frac{\ell \cdot L \cdot \mathsf{MaxTrial}}{n2^n} \leq \epsilon_{\mathsf{sec}}$ を満たす自然数とする．また $k_i (1 \leq i \leq L)$ は i 番目の平文の暗号化・暗号文の復号に用いられる $\ell+2n$ ビットの鍵である．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．

4.3.2　平文の送信

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_S に基づいてインデックス $idx \leftarrow \mathsf{GetIdx}_S(t_s)$ を計算し，$\mathsf{Snd}(k, s, idx)$ を実行する．Snd は，入力 $k = (k_1, \ldots, k_L)$, s および idx から以下のように暗号文 $m \in GF(2^\ell) \times GF(2^n)$ を生成する．ただし，以下における認証子生成関数 A は式 (1) で定義したものである．

$\mathsf{Snd}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}(k, s, idx)$
1. $(k_S, k_A) \leftarrow k_{idx}$
2. $c \leftarrow s + k_S$
3. $a \leftarrow A(k_A, c)$
4. **output** (c, a)

4.3.3　暗号文の受信

暗号文の受信にあたり，受信者は送信者と同様，オラクル $\mathcal{O}_{\mathsf{GNS}}$ にアクセスする．次に得られた時刻情報 t_R からインデックス $idx \leftarrow \mathsf{GetIdx}_R(t_R)$ を計算し $\mathsf{Rcv}(k, idx)$ を実行する．Rcv は，入力 $k = (k_1, \ldots, k_L)$ から復号に用いる鍵 k_{idx} を取り出し，復号処理を行う．提案方式ではノイズを含み，揺らぎのある通信路 C からを暗号文を抽出するために，C から暗号文長分のデータ $m = (c, a)$ を抽出し，認証子生成関数 A で受理される正しい (c, a) を抽出するビットの位置をずらしながら探索する．このようにし

[*3] $\mathsf{GetIdx}_S, \mathsf{GetIdx}_R$ の実現可能性については 5.2 で検討する．

て暗号文を抽出することにより，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．擬似コードは以下のようになる．ただし以下のコードにおいて o は前回の Rcv 実行時の最後のオフセット値が格納されているものとする．

$\mathsf{Rcv}_{\mathsf{C}}^{\mathcal{O}_{\mathsf{GNS}}}(k, idx)$
1. $(k_S, k_A) \leftarrow k_{idx}$
1. $o \leftarrow o + \ell + n$
2. $c \leftarrow 0$
3. **while** $(cnt < \mathsf{MaxTrial})$ **do**
4. $(c, a) \leftarrow \mathsf{C}[o : o + \ell + n]$
6. **if** $a = A(k_A, c)$ **output** $c + k_S$
7. $o \leftarrow o + 1$
8. $cnt \leftarrow cnt + 1$
9. **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，提案方式の正当性を保証することが可能となる．

紙面の都合上証明は省略するが，上述の方式の安全性は以下の定理で表される．

定理 1 4.3 に記載の方式 $(\mathsf{Gen}, \mathsf{Snd}, \mathsf{Rcv})$ は $\frac{\ell \cdot \mathsf{MaxTrial}}{n2^n}$-正当性，$\frac{\ell \cdot L \cdot \mathsf{MaxTrial}}{n2^n}$-偽造不可能性，および完全秘匿性を満たす．

4.4 小型衛星向けセキュア通信方式 [16]

小型衛星向けセキュア通信方式も前節で提案したロケット向け通信と同じ秘匿機能付き認証コードを用いる．ただし，衛星では GNSS 受信機を搭載しているとは限らないため，小型衛星向けの通信方式は鍵の同期に時刻情報を利用しないものとなっている．具体的には，ロケット向け通信が，送信する平文 s を直接，秘匿機能付き認証コードで暗号化して送信するのに対し，小型衛星向け通信方式では送信する平文 s にインデックスヘッダ idx を付与したデータを秘匿機能付き認証コードで暗号化する．ここで新たに導入された idx は，ここで idx は，共有鍵 $k = (k_1, \ldots, k_L)$ から秘匿機能付き認証コードに用いる鍵 k_{idx} を導出するために用いるデータとなる．この方式では，オフセットヘッダ部を暗号化してしまうと秘匿機能付き認証コードに用いる鍵を導出することができなくなるため，オフセットヘッダ部は平文のまま送るが，攻撃者により改竄されない形で送る必要がある．具体的な方式は以下のようになる．

4.4.1 鍵生成

ロケット向け通信と同一.

4.4.2 平文の送信

平文 s の送信にあたり，Snd は鍵 $k_{idx} = (k_S, k_A)$ なる k_S を用いて s を秘匿し，さらに k_A を用いて (idx, s) の改竄防止を行う．具体的には平文 s の暗号化処理は次のようになる．

$\mathsf{Snd}_{\mathsf{C}}(k, s, idx)$
1. $(k_S, k_A) \leftarrow k_{idx}$
2. $c \leftarrow s + k_s$
3. $a = A(k_A, (idx, c))$
4. **output** (idx, c, a)

4.4.3 暗号文の受信

$\mathsf{Rcv}_{\mathsf{C}}(k, \mathsf{C}, idx)$ は $k_{idx} = (k_S, k_A)$ を用いて通信路 C から暗号文を取り出し，得られた (idx, c, a) の (c, a) を k_S により復号する．通信路からの暗号文の抽出は，ロケット向け方式と同様，通信路から暗号文の候補を 1 ビットずつずらしながら検証することで実現する．

この方式を単純に運用すると過去の暗号文を再送するリプレイ攻撃が可能になる．そこで提案方式では，送信のたびにインデックスを単調増加させ，受信者ではオフセットヘッダの値が過去に受理したインデックスよりも大きい値であることを確認することが必要となる．

紙面の都合上証明は省略するが，上述の方式の安全性は以下の定理で表される．

定理 2 4.4 に記載の方式 $(\mathsf{Gen}, \mathsf{Snd}, \mathsf{Rcv})$ は $\frac{\ell \cdot \mathsf{MaxTrial}}{n2^n}$-正当性，$\frac{\ell \cdot L \cdot \mathsf{MaxTrial}}{n2^n}$-偽造不可能性，および完全秘匿性を満たす．

5. プロトタイプ実装および評価実験

文献 [16] では認証子生成演算が実用上問題ない速度で行えることを確認できた．方式の実利用に向け，プロトタイプ実装を行い，地上での実証実験を行った結果を本節で示す．なお，宇宙機に搭載した実証実験は今後の課題である．

5.1 実装に用いた認証子生成演算とその性能

プロトタイプ実装にあたっては，$GF(2^{128})$（既約多項式 $x^{128} + x^7 + x^2 + x + 1$）上の A-code を用いることにした．既約多項式の選定基準は，文献 [16] と同様，実装高速化のために (1) 項数が少なく，かつ (2) 低次に非零の係数があることである．この A-code を，ローエンド FPGA である Intel MAX10 10M50SCE144I7G に実験用回路（時刻カウンタなど）とともに実装した．A-code 単独での演算クロック数は 1 クロック，最高動作周波数は 107.68MHz，スループットは 13.78Gbps，回路規模は 11751LE であり，ロケットや衛星の無線通信速度と比べはるかに高速である．文献 [16] では異なる品番の FPGA で実装評価を行っているが，それと同水準の結果である．

5.2 提案方式における鍵同期の実現可能性

ここでは，4.3 の方式においてロケットと地上局で同じ鍵を用いるために仮定している同期機構の実現可能性を検証する．

GNSS 受信機の多くは時刻情報とともに 1 秒周期の時刻

パルス（1PPS 信号）を出力できる．二つの受信機間でのパルスずれ，すなわち同期ずれは 1 マイクロ秒以内（実測 100 ナノ秒程度）の仕様である場合が多い．宇宙機用の GNSS 受信機も存在し，同様の仕様である [11]．

しかし GNSS 受信機どうしが同期していても，各々を持つ宇宙機と地上局が無線を仲介して時刻同期を保てるかは実証を要する．そこで今回，時刻情報の無線伝送実験を行った．GNSS 1PPS 信号で補正した時刻カウンタを二つ用意し，一方の値を他方に無線伝送して送信時刻と受信時刻を記録し，時刻差の揺らぎを測定した．

実験環境は次のとおりである（図 1）．時刻カウンタ値と位置情報（計 128 ビット）に A-code (128 ビット) を付加したパケットを送る送信機と，パケットを受信し自分の時刻値とともに記録する受信機を，それぞれ FPGA 上に実装した．そのうえで，小型ロケット射点に送信機を設置し，受信機を地上局（距離約 600m）へ向け移動しながら遠ざけた（図 2）．無線送受信には市販の IoT 用 920MHz 帯特小無線機（Lora）二種類，ES920LR モジュール（EASEL 製，出力 20mW）と IM920S モジュール（インタープラン製，10mW）を用いた．そして，提案方式と同様の一方向通信とするため，ブロードキャストモードでパケットを送出した．

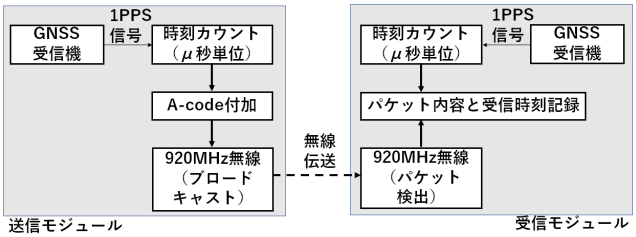

図 1 時刻同期の評価実験環境

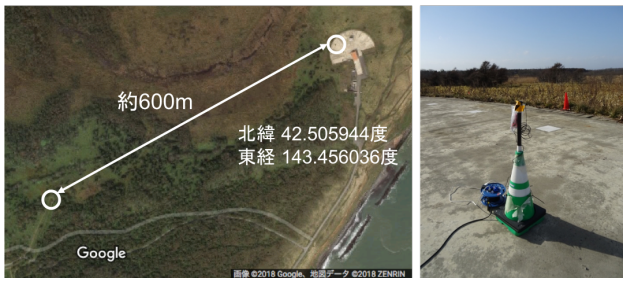

図 2 時刻同期の評価実験場所

測定結果を図 3 に示す．信号強度によらず時刻差の揺らぎは 4 ミリ秒以内に収まっているため，鍵読み出し周期が 250Hz 以下（コマンド無線などには十分）であれば，鍵のずれは高々前後 1 周期に留まると考えられる．したがって，三つの鍵を試すことで鍵の同期が行えることが実証された．

また，時刻差が大きく，信号受信強度との相関も低いことから，変動は電波到達時間など自然現象に由来するものではなく，Lora モジュールの内部処理に由来すると推定される．フライトで実際に用いる無線系では変調方式や下位プロトコルはほぼ自由に決定できるので，遅延変動はより低く抑えることができ，高速な交信にも対応できると期待される．

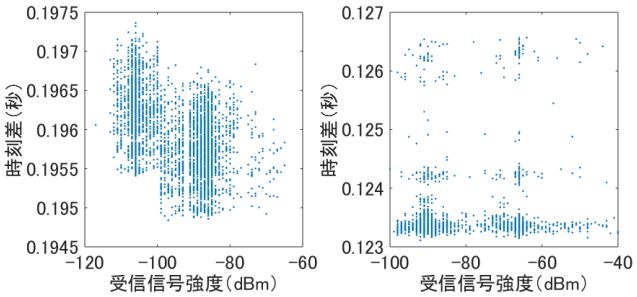

図 3 時刻差の揺らぎ（左：ES920LR，右：IM920S）

5.3 暗号文抽出の実現可能性

受信ビットストリームから，A-code の検証による暗号文抽出の実現可能性に関する基礎調査を行った．図 4 に実験環境を示す．無線部分には 433MHz 帯 RF モジュールを使用した．送信機（FS1000A，出力 10mW）はディジタル 2 値信号を入力として AM 変調と送信を行い，受信機（RXB6）は復調した 2 値信号を出力する．誤り訂正やパケット抽出などのアルゴリズム処理は実装されていない．

作成した送信ユニットは，A-code 付パケットを生成して 1 ビットずつ無線機へ転送する．受信側では無線機出力をサンプリングしてシフトレジスタに蓄積し，1 ビットシフトしながら A-code 比較を行って，A-code が合致した場合にパケットとして出力する．送信ユニットと受信ユニットは室内で約 10cm の距離に設置した．

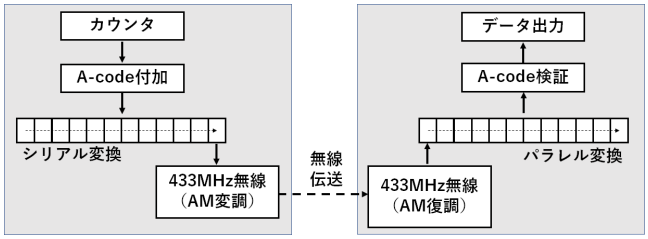

図 4 通信データ特定の評価実験環境

実験の結果，最大 11.1kbps（無線機のほぼ最大速度）で全てのパケットを検出でき，パケット消失や誤検出は 1 時間のロングラン中発生しなかった．これにより，提案方式による通信データ特定が基本的に可能であることを確認できた．通信速度については無線機の変更で向上すると思われる．

5.4 他主要箇所の実現可能性

今回評価実験を行っていない主要箇所について，実現可能性は文献 [16] と同様以下のとおりである．

5.4.1 鍵ストレージ

オンボードの鍵ストレージとしてフラッシュ・メモリを想定する．必要な最低容量は，ロケットで数百 M バイトと推定される[*4]．衛星ではミッションによる違いが大きいが，数百 G〜数百 T バイトと推定される[*5]．したがって制御信号や小量ミッションデータであれば，現在入手可能なメモリカードや SSD で足りる．ストレージデバイスの放射線耐性についても調査が進められており [13]，実現性に大きな支障はない．

5.4.2 乱数生成機構

物理乱数による高速真性乱数生成方式などが研究されており [14]，様々な乱数生成デバイスも開発されている．

6. おわりに

本稿では，文献 [16] で行われた衛星・ロケットと地上局との通信システムを対象とた，脅威分析，および定性的なセキュリティの整理を踏まえ．暗号理論的にフォーマルなセキュリティモデルの提案を行った．また提案したセキュリティモデルに基づき，文献 [16] で提案した二つの方式が数学的に証明可能であることを示した．また，プロトタイプ実装では，文献 [16] で FPGA 実装した方式の演算部と，無線通信機器，GNSS 受信機を組み合わせたより本番環境に近いシステムを構築し，4.3 に記した方式の地上実験を行うことでその有効性を確認した．以上の結果により，文献 [16] で示唆した小型衛星・ロケット用通信における情報理論的安全性の達成がさらに一歩前進したこととなる．

今後の課題として，ライフタイムの長期化に伴う鍵数の増加対策として，地上局—衛星間の量子鍵配送 [10] を利用した飛行中の鍵共有や，鍵の再利用も含めた柔軟な運用可能性を検討し，状況に応じて計算量的安全性への切り替えも可能にすることが挙げられる．また，提案方式の詳細設計と実装を進め，フライトテストなどを通して有用性を実証することも挙げられる．

参考文献

[1] 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

[2] 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.

[3] 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

[4] 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

[5] C.E.Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal, vol.28-4, pp.656–715, Oct. 1949.

[6] 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.

[7] G.J.Simmons, Authentication Theory / Coding Theory, Proceedings of CRYPTO 1984, LNCS, Vol. 196, Springer Verlag, pp. 411–431, 1984

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] B. den Boer, A Simple and Key-Economical Unconditional Authentication Scheme, Journal of Computer Security, Vol. 2, pp. 65–71, 1993.

[13] 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.

[14] V.Fischer and P.Haddad, Random Number Generators for Cryptography, Chapter 7, Circuits and Systems for Security and Privacy, CRC Press, 2016.

[15] Luke McAven, Reihaneh Safavi–Naini, and Moti Yung, Symmetric Authentication Codes with Secrecy and Unconditionally Secure Authenticated Encryption, Proceedings of INDOCRYPT 2004, LNCS, Vol. 3348, Springer Verlag, pp. 148–161, 2004.

[16] 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.

[*4] データレート 100kbps，打ち上げ準備から衛星分離まで 10 時間と仮定して総平文量は約 450M バイト．

[*5] データレート 10Mbps, フライト期間 1 年，可視範囲 1/10 と仮定して総平文量は約 4T バイト．