3-4　ドローンを用いた動画秘匿伝送

西澤亮二　市原和雄　伊藤寿之　藤原幹生　佐々木雅英

量子 ICT 先端開発センターは、平成 28 年 4 月 12 日に秋田県仙北市で実施のドローンによる図書の自動配送実証実験において、物理乱数列を用いたワンタイムパッド（One-Time Pad：OTP）暗号により、ドローンの制御通信を高秘匿化することを成功させていた [1][2]。これに続き、暗号化されたドローン撮影動画を撮影用とは別の中継用のドローンを介して地上局に中継する技術を開発、平成 29 年 2 月にその実証実験を成功させた。実験は、野外における施設監視を想定した屋外実験と、建屋内での捜索を想定した屋内実験を実施した。本稿では技術開発の内容を中心に、この実験の様子も併せて述べる。

1　開発経緯

当センターでは、既に、ドローンの OTP 暗号化した制御通信の実証実験を成功させていた。ドローンの制御通信は毎秒数百 Kbit と低速度であり、OTP 暗号による高秘匿化を比較的容易に実装できるものであった。一方、ドローン間あるいはドローンと地上局間での動画など大容量データの通信は、毎秒数 M ～数十 Mbit の高速通信となる。このため、これと同じ長さの大量の乱数列を用意し、かつ、これら大量の鍵を同期させる技術が必要となる。また、ドローンによる動画撮影は、重要施設の監視や大規模イベントでの警備の用途が想定されるが、その際、移動範囲が広範となることから、中継機を介した動画中継技術も必要となる。そこで、これらの技術に焦点を当てた開発を行うこととした。

2　OPT 暗号化と真性乱数

OTP 暗号化とは、真性乱数列を暗号鍵として送受信者間で秘密裏に共有、平文を暗号鍵との排他的論理和（XOR）によって暗号文を生成して送信し、受信側で共有した暗号鍵の XOR によって復号するという方法である。その際、暗号鍵は剥ぎ取り式メモ（パッド）のように使い捨てる。この方法は、現在知られている暗号プロトコルで唯一、情報理論的安全性が証明されており [3]、またデータ（平文）と同じサイズの真性乱数列さえ共有できれば、暗号化・復号の処理は単純な XOR 計算なので計算遅延を生ずるおそれもない。

小型物流用ドローンは積載量 5 kg 程度、バッテリー持続時間 20 分程度のもので、搭載する計算機サイズも制限される。現在普及の公開鍵暗号は、その安全性を計算能力に依存しており、限られた計算能力では計算遅延やそれに起因する電波干渉などにより通信劣化を招くおそれがある。また、暗号装置の安易な軽量化は、高い計算能力を持つ計算機による解読の危険性を高めてしまう。上記の OTP 暗号化を用いれば、供給した真性乱数列を使い切るまでの間は、情報理論的安全性を持ったセキュアな通信を、計算能力の制限を受けることなく行うことができる。

なお、真性乱数列とは規則性も再現性もない完全にランダムな数字の系列である。熱雑音や量子力学的現象など、予測不可能な物理現象を利用したデバイスによって生成される物理乱数が、この特徴を持つとされる。物理乱数には、このような生成方法に起因した生成速度の限界があるため、一般の暗号通信では確定的な計算アルゴリズムによって生成される疑似乱数を用いることが多い。しかし、疑似乱数列には必ず周期性があり、高い計算能力を持つ計算機により解読されてしまう危険がある。情報理論的安全性を有する通信の実現には真性乱数は必須である。

OPT 暗号化では、伝送するデータ量と同じサイズの真性乱数列が必要となるが、ドローンの飛行時間は限られているため、その通信の暗号化に必要な量を小型のメモリに蓄えておくことは十分に可能である。また、暗号化と復号は、データあるいは暗号文と暗号鍵の XOR で済むので計算遅延が極めて小さく、物理的な回路構成、暗号処理時間ともに非常に軽量かつ低コストの実装が可能である。あらかじめ通信端末間で真性乱数列を共有しておく必要はあるものの、その際に真性乱数列を用いた機器認証を行うことで、不正なドローンによる暗号鍵の窃取を排除することができる。この機器認証では、通信機器間で共有したメッセージ（真正乱数列）をハッシュ関数[*1]で演算して得たメッセージ認証コード[*2]が一致する場合に、真正な機器であると認証するというメッセージ認証を応用した方

式をとっている（Wegman-Carter 認証方式 [4]）。さらに、強力ななりすまし防止機能を持たせるため、共有メッセージを真性乱数列、ハッシュ関数も真性乱数列より生成し、かつ認証を機器間相互で行っている。

3　動画データ中継

撮影ドローンでは、監視カメラから入ってくる動画データのパケット（ビット列）に暗号鍵を XOR して暗号文を生成し、中継ドローンへ伝送する。中継ドローンは、暗号化された動画データを指向性アンテナで受信し、復号せずにそのまま地上局に中継する。地上局は、受信した暗号文に暗号鍵を足し算して動画データを復号する（図 1）。

データ中継には、安価で無線局免許不要な市販 Wi-Fi 機器（Buffalo 社製 Air Station Pro WAPS-AG300 H：指向特性水平面 60 ± 5°、垂直面 65 ± 5° の指向性セクターアンテナ WLE-HG-DA/AG 付き：IEEE 802.11 b/g 準拠）を使用し、一般的な屋外 Wi-Fi 電波（2.4 GHz 帯）により、低コストかつ容易な方法で電波の届かないエリアでの秘匿動画中継を実現することとした（図 2）。

撮影ドローンと地上局は、あらかじめ離陸前に真性乱数列を暗号鍵として共有しておき、制御通信やデータ通信をパケットごとにワンタイムパッド暗号化して通信を完全秘匿化する。ドローン通信では通信路の特性変動が大きくデータ欠損も頻繁に生じるため、大量の暗号鍵をドローンと地上局間でパケットごとに正確に同期させ、正しく更新する仕組みが必要となる。今回は、通信路特性に応じて最適なパケット間隔で鍵同期信号を送信する技術を開発した。これにより、データ伝送効率の低下を最小限に抑えつつ鍵同期を行い、次々に新しいカメラ映像を低遅延で送り続けることが可能となった。

4　通信パケット構造

撮影カメラから送られる動画の圧縮方式は H.264（動画ファイル形式 MPEG の一種）で、毎秒 15 枚の画像（毎秒 1 枚伝送される基準フレームのサイズは 320 × 240 pixel）で構成される。動画データの伝送速度は毎秒 12 Mbit と比較的高速であるが、1 回の実験での撮影と伝送は 15 分程度であり、そこで必要な真性乱数列のサイズは約 11 Gbit となる。

ドローン通信では通信路の特性が変動しやすく、データ欠損も頻繁に生じるため、動画データの秘匿伝送のためには、大量の真性乱数列をドローンと地上局間で正確に同期させる仕組みと、パケットごとに暗号

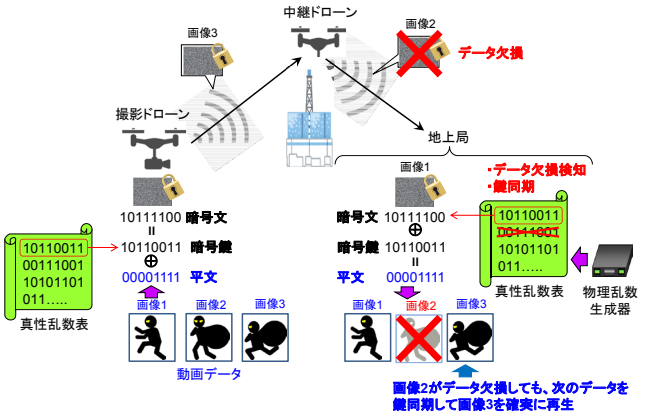

図 1　完全秘匿データ中継の仕組み

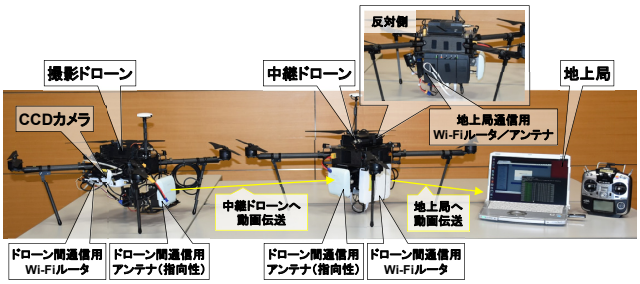

図 2　構成機器類の外観写真
（左：撮影ドローン、中央：中継ドローン、右：地上局）

鍵を正しく更新する仕組みが必要となる。そこで、データ伝送中のパケット損失に対応するため、通信路特性に応じて最適なパケット間隔で鍵同期信号を送信する技術を開発した。また、監視画像では監視対象のリアルタイムでの捕捉が要求されることから、今回の実験では、OSI 参照モデルの第 4 層（トランスポート層）でのプロトコルに UDP（User Datagram Protocol）を用いて欠損したデータの再送はせず、次に来るデータで鍵同期することで、可能な限りリアルタイムに動画再生をするようにした。また、長時間（1 秒程度）のデータ欠損があっても鍵同期を確保するため、通信路特性に応じ最適なビット間隔（今回の実験では 32 Mbit 間隔）で鍵同期信号を送信し、送受信者間での鍵同期を保証できるシステムとなっている。

大まかなパケット構造を図 3 に示す。撮影された動画は 2,048 bit ごとに分割したうえで同サイズの真性乱数列と XOR し、それぞれに 8 bit の識別用 ID ヘッ

＊1　ハッシュ関数とは、入力されたデータから固定長の短いコード（ビット列）を出力する一方向関数。同じ入力であれば必ず同じコードを出力する。

＊2　メッセージ認証コード（Message Authentication Code：MAC）とは、送信されたメッセージが改ざんされていないことを認証するための固定長の短いコード。メッセージをハッシュ関数により演算することで得る。

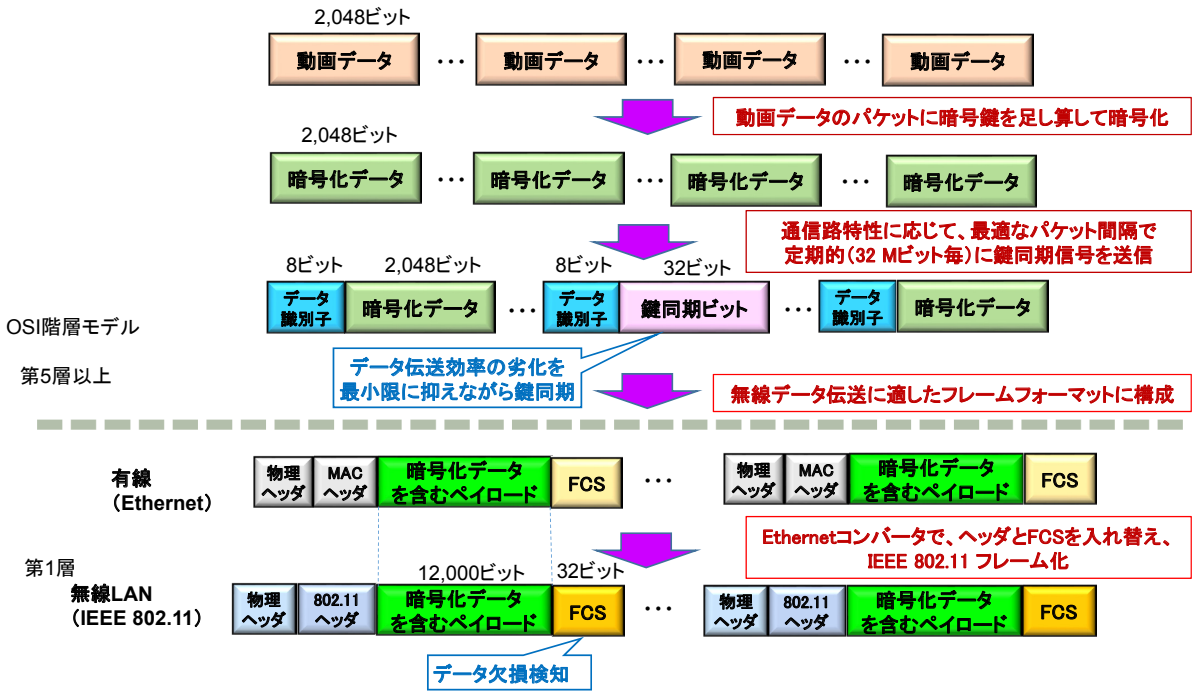

図３　データ欠損が生じる場合における動画データのワンタイムパッド暗号化手法の概要

図４　完全秘匿データ中継技術を実装したドローンによる監視業務模擬実験。地上局－中継ドローン－撮影ドローン、の位置関係。挿入図は地上局における受信動画。

ダを付ける。ここで 32 Mbit ごとに 32 bit の鍵同期信号を挿入する（この信号にも同様に識別用 ID ヘッダを付す）。これらをペイロードとして、トランスポート層以下でパケット化する。なお、パケットは、Ethernet フレームフォーマットに準じた MAC フレーム*3 とし、無線で伝送する際に Ethernet コンバータにおいて、MAC ヘッダを外したうえで IEEE 802.11 に準じたカプセル化を行う。無線通信時のパケット損失等によるデータ欠損は、このカプセル化の際に付された 32 bit の FCS（Frame Check Sequence）で検知される。

上記鍵同期信号で真性乱数列の同期ずれを随時補正することにより、データ伝送効率の低下を最小限に抑えながら正確に OPT 暗号化を行い、次々に新しいカメラ映像を低遅延で送り続けるようにした。また、データ欠損が検知された場合には、データの再送要求をしないでそのパケットの復号は行わずに次のパケットの復号に移ることとし、被写体の動きを見逃すことなく、監視カメラからのデータを受信し続けることを可能とした。

5　屋外フィールド実験

2017 年 2 月 22 日（水）に愛知県豊田市郊外の屋外テストフィールドで行った実験は、ドローンによる上空からの監視業務を模擬し、不審者に扮した人（被写体）を追う撮影ドローンからの映像を、中継ドローンを介して地上局で受信するという状況で行った（図 4）。

実験は 1 回 15 分程度のものを数回実施した。撮影ドローンは、監視対象区域でありながら樹木などにより地上局から直接見ることができない位置まで飛行し、不審者を撮影した暗号化された動画データを 50 ～ 100 m 離れた中継ドローンに伝送する。中継ドローン

＊3　MAC (Media Access Control) フレームとは、Ethernet で送信先アドレスなどの制御情報を付加した小さな一群のデータのこと。Ethernet ではフレーム単位でデータがやり取りされ、そのサイズは 514 ～ 12,144 bit である。

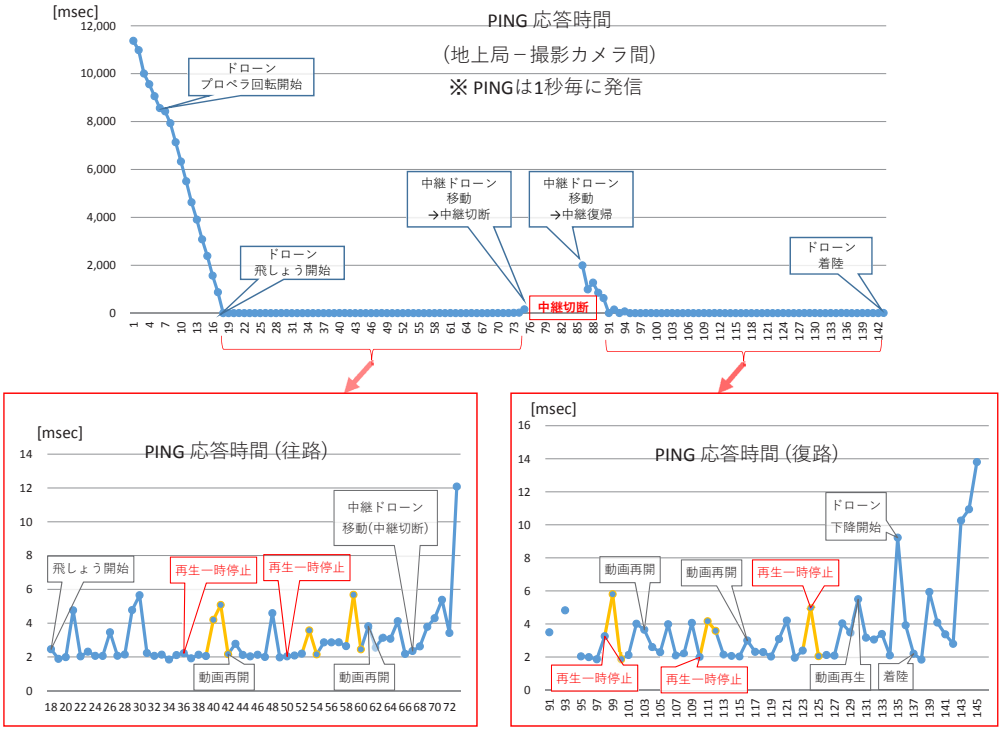

図５　地上局－撮影カメラ間の PING 応答時間 (横軸は PING 信号に付した連番)

は、動画データを指向性アンテナで受信して、約 10 m 離れた地上局に中継、地上局は撮影ドローンと同じ暗号鍵を用いて動画データを復号し動画再生する。監視カメラの動画データを完全秘匿化したまま中継伝送するという想定で実験を実施した。

また、中継の切断を模擬するため、敷地境界（図４上端）まで撮影ドローンが移動したところで、ドローン間通信が森林帯によって妨げられるように中継ドローンを移動させた（図４左端）。なお、実施にあたっては、実験場の管理者である愛知県豊田市の許諾を頂いた（ドローンの制御については、１機につき必ず操縦者１名を配し、目視外飛行や不慮の墜落等のインシデントが発生しないよういつでも手動介入できるよう配慮した）。

地上局-撮影ドローン間の通信状況は、地上局での再生動画をハンドカメラで撮影するほか、地上局から動画撮影カメラに対して１秒ごとに発信される PING[*4] の応答時間を記録する方法で観察した。また、再生動画のほか、実験自体の様子もハンドカメラで撮影している（NICT プレスリリース『ドローンによる動画データの完全秘匿中継技術を開発』参照：http://www.nict.go.jp/press/2017/03/22-1.html）。

地上局での動画再生はリアルタイムかつ「コマ落ち（画像データが失われること）」することなくスムースに行われた。このことから、本実験での機器構成において、動画中継及び暗号化・復号がほぼ問題なく機能することが確認された。また、中継ドローンを森林帯の陰に移動させ中継の切断を模擬した際には、地上局での動画再生は停止し、PING 応答も完全に途絶えてしまったが、中継ドローンを元の中継位置に戻したところ、PING 応答も再び確認され、中継切断中の映像を飛ばした状態で動画再生が再開された。このことから、暗号化された動画データの伝送が途切れたとしても、定期的に挿入された鍵同期信号により送受信側で暗号鍵を一致させて暗号化データが復号されることが確認された。

なお、動画中継自体はほぼ問題なくできたが、撮影ドローンがある地点（図４中央付近の車両前後）を通過する際、必ず動画再生が５秒程度一時停止し、コマ落ちなしで動画再生が復活するものの早回しのように再生されてしまうという現象が生じた。車両鉄板で通信電波が反射し干渉性フェージング[*5] が起きて動画データの伝送に遅延が生じたと推測し、車両を実験エリアから移動させて中継実験を行ってみたが、同様の

＊4　PING とは、IP (Internet Protocol) ネットワークにおいて、ノードの到達性を確認するための標準装備ソフトウェア。指定した相手先に一定サイズのパケットを送り、その戻りの有無によりネットワークの接続を確認する。応答速度も表示されるため、ネットワークの速度を確認することもできる。潜水艦が水中で発するアクティブ・ソナーに挙動が似ていることから、その音（“ping”）に由来して名付けられた。

＊5　干渉性フェージングとは、送信点から受信点に届く電波の経路が、物体による電波反射が原因で複数ある場合、それぞれの伝播経路の長さが違うことで受信点においてそれぞれの位相がずれ、強め合ったり弱め合ったりすることにより無線局での電波の受信レベルが変動する現象。電波の受信ができなくなる場合もある。

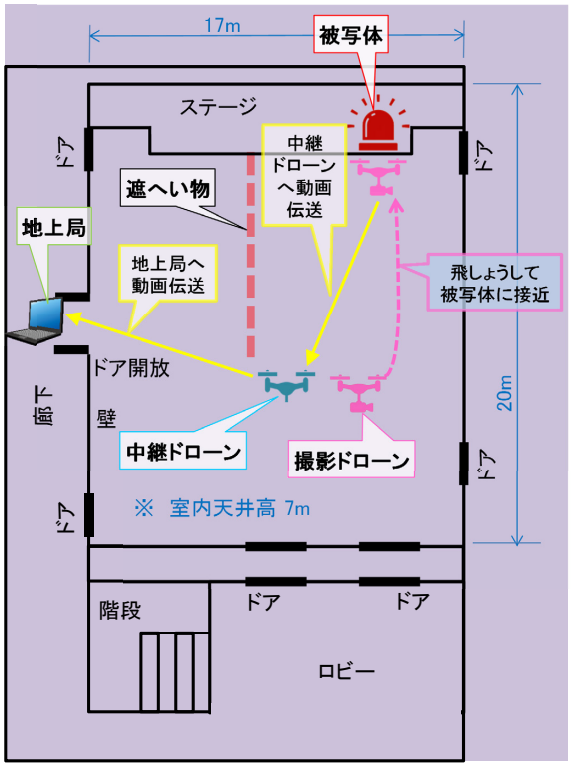

図 6　屋内実験の機器位置関係。各ドローンに手動介入のための監視者を配置（地上局と中継ドローン間、各ドローン間の距離はいずれも約 10 m）

結果を得た。このことから、同地点では、車両の影響ではない何らかの理由で通信に遅延が生じていたと推測される（実際、動画再生の一時停止が見られる際には、必ず PING 応答時間に若干の上昇がみられた：図 5）。

当該テストフィールドの 200 ～ 300 m 近傍に携帯電話基地局が 3 基あるが、その影響を含め、今後このような現象につき改めて調査することとしたい。

6　屋内実験

平成 28 年 2 月 26 日（日）に東京都小金井市の NICT 本部 4 号館講堂（20 m × 17 m × 天井高 7 m）で実施した実験は、災害により倒壊危険が生じた重要施設内での探索業務を模擬し、室外の地上局から視覚的に隔離された撮影ドローンで取得した画像データを、中継ドローンを介して、地上局で受信するという状況で行った（図 6）。

実験は、1 回 10 分程度のものを数回実施した。建屋内を撮影ドローンによって探索するというシナリオの下、ドローン間及び中継ドローンと地上局間の距離は、共に約 10 m と近距離としつつ、さらに、撮影ドローンと地上局間にパーティション（幅 7.8 m × 高さ 1.8 m）を設置し、地上局へは撮影ドローンからの電波が直接届かないという想定で実験を行った。暗号化された動画データ通信と動画再生手順について屋外フィールド実験と同様に実施したが、あくまで室内での通信状況を確認するという目的の下、中継切断の実験は行わなかった。

地上局–撮影ドローン間の通信状況については、室内環境でもしっかりとデータ伝送ができ、動画再生ができるかという点のみ確認するものとして、地上局での再生動画をハンドカメラで撮影する方法でのみ観察した。また、再生動画のほか、実験自体の様子もハンドカメラで撮影している（NICT プレスリリース『ドローンによる動画データの完全秘匿中継技術を開発』参　照：http://www.nict.go.jp/press/2017/03/22-1.html）。

地上局での動画再生は、リアルタイム、かつコマ落ちすることなくスムースに行われ、上述の屋外実験とは異なり、動画再生が一時停止するという現象も生じなかった。これにより、室内環境においても、暗号化・復号及び動画中継がほぼ問題なく機能することが確認された。

7　今後の展望

今後は、暗号化・復号装置をよりコンパクトかつ信頼性の高いものとする開発を進める。また、今回用いた機器構成によるデータ伝送によりどのような電波強度分布となるか、無反響室などにおいて通信実験を実施・検証し、よりよい中継技術の開発に活かす。さらに、人の立ち入るのが難しい重要施設の監視などへ活用するために信頼性試験を継続するとともに、撮影・中継ドローンの台数を増やし、広域で多様な中継ネットワークを柔軟に構成するための技術開発にも取り組んでいく。

【参考文献】

1　伊藤寿之ら“ドローン通信システムの安全性強化とその応用,”2016 年電子情報通信学会基礎・境界ソサイエティ・NOLTA ソサイエティ大会, AI-3-5, SS-33, 2016 年 9 月
2　伊藤寿之ら“高秘匿ドローン通信ネットワーク,”2017 年電子情報通信学会総合大会, AI-3-2, SS-50, 2017 年 3 月
3　C. E. Shannon, “Communication Theory of Secrecy Systems,” Bell System Technical Journal, vol.28 (4) , pp.656–715, 1949.
4　M. N. Wegman and J. L. Carter, “New hash functions and their use in authentication and set equality,” Journal of Computer and System Sciences, vol.22, no.3 pp.265–279 (1981) .

西澤亮二　（にしざわ　りょうじ）
未来 ICT 研究所
量子 ICT 先端開発センター
研究技術員
ドローン通信

市原和雄　（いちはら　かずお）

株式会社プロドローン
常務取締役
ドローン制御、通信

伊藤寿之　（いとう　としゆき）

未来 ICT 研究所
量子 ICT 先端開発センター
研究員
博士（地球環境科学）
物理レイヤ暗号、光空間通信

藤原幹生　（ふじわら　みきお）

未来 ICT 研究所
量子 ICT 先端開発センター
研究マネージャー
博士（理学）
量子鍵配送、光子検出技術、極低温エレクトロニクス

佐々木雅英　（ささき　まさひで）

未来 ICT 研究所
主管研究員
理学博士
量子通信、量子暗号