東京大学
THE UNIVERSITY OF TOKYO

PRESS RELEASE

2023 年 1 月 11 日

東京大学国際ミュオグラフィ連携研究機構

世界初、ミュー粒子によるワイヤレスセキュリティ技術

１．発表のポイント：

◆ 暗号鍵を送受信者間で一切やりとりしない超高セキュリティワイヤレス通信技術の開発に成功した。
◆ 次世代近距離通信におけるデータエンコード標準技術として期待される。
◆ 強固な暗号化技術としてポスト量子暗号学に寄与することが期待される。

２．発表概要：

東京大学国際ミュオグラフィ連携研究機構は、送受信者間で暗号鍵（注１）のやりとりを一切必要としないしない全く新しいタイプの超高セキュリティワイヤレス通信技術「COSMOCAT」の開発に成功した。宇宙線ミュー粒子（注２）の到着時刻の極めて高い任意性（注３）を用いて送信者は極めて強固な暗号鍵を生成することができ、宇宙線ミュー粒子の飛行速度の普遍性（注４）から受信者は送信者の暗号鍵を高い精度で推定できる。その結果、ワイヤレス通信において極めて高いセキュリティを実現する。

暗号鍵として用いるのは真性乱数（「次に何が来るのか、真にわからない」乱数）であり、量子コンピュータ（注５）を用いても容易に解読できるものではない。また、物理的な暗号鍵のやりとりをしないため、ハッキングも不可能である。近い将来、同技術は特に次世代近距離通信（注６）において活用されると期待される。

３．発表内容：

＜COSMOCAT について＞

ミュー粒子は、銀河系における超新星爆発などの高エネルギーイベントによって加速される宇宙線と、地球大気が反応してできる素粒子の一つである。ミュー粒子は透過力が強く、あらゆる人工構造物をほぼ真空中の光速度で貫通することができる。また、銀河系の磁場に何百万年間もの間捕捉され続けてきた宇宙線が少しずつ地球に染み出してきてミュー粒子が生成されることから、ミュー粒子の地球への到着時刻は真性乱数である。送信者はミュー粒子を検出することで、その検出時刻を暗号鍵として文書をエンコードする。一方、受信者は同一のミュー粒子を別の場所で検出することでその検出時刻を保存する。受信者は送受信者間の距離からミュー粒子の飛行時間を正確に計算することができるので、暗号鍵の物理的なやりとりなく、文書をデコードすることができる（図１）。更に、ミュー粒子が地表へ到着するタイミングには極めて高い任意性があり、到着時刻をピコ秒精度で記録することで、到着時刻そのものを

10 桁以上の真性乱数から成る暗号鍵として取り扱うことが可能である。ミュー粒子の速度は屋内、屋外、地上、地下問わず同じ速度が担保されているので、地球上いかなるところでも COMOCAT を実施することが可能である。

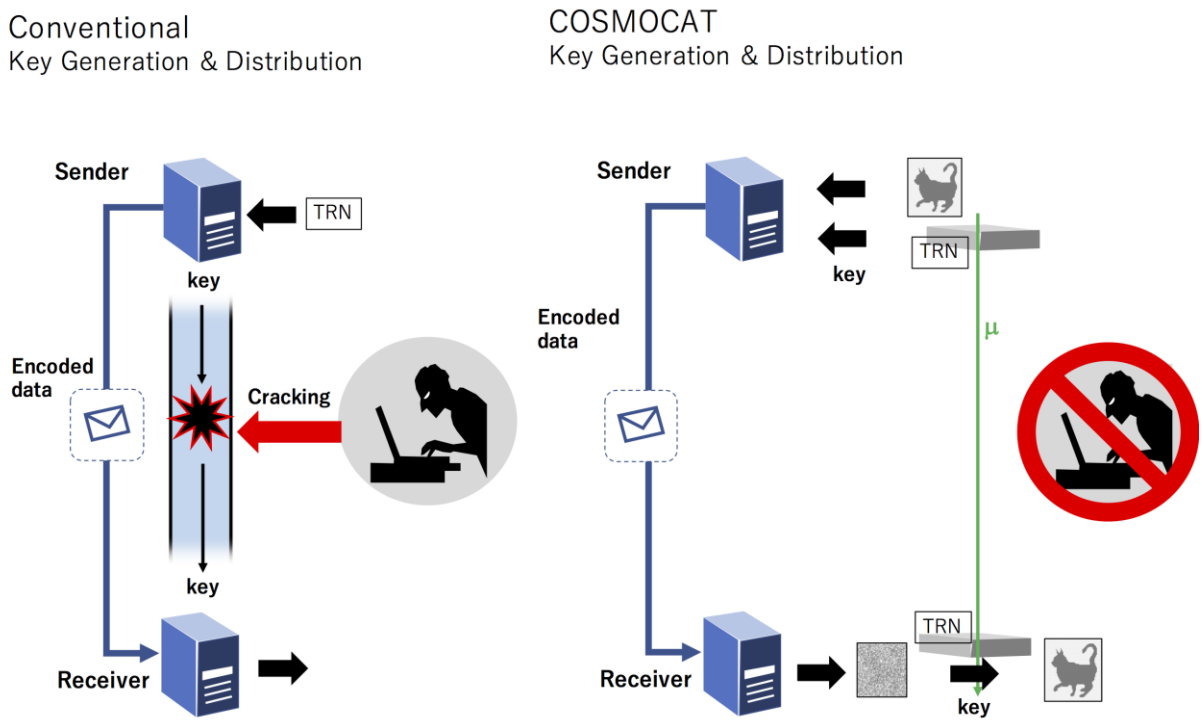

図１：COSMOCAT の原理

図２には COSMOCAT の応用例が示されている。現在、スマートビルディング（注７）や空間伝送型ワイヤレス電力伝送システム（注８）が、近未来技術として普及しつつある。このようなシステムで用いられる次世代近距離通信においてはセキュリティがほとんど考慮されておらず、ビル内インフラのハッキングや電気窃盗などが起きやすい状況となっている。COSMOCAT による暗号化通信を活用することで、近距離通信において極めて高いセキュリティを担保できるようになる。

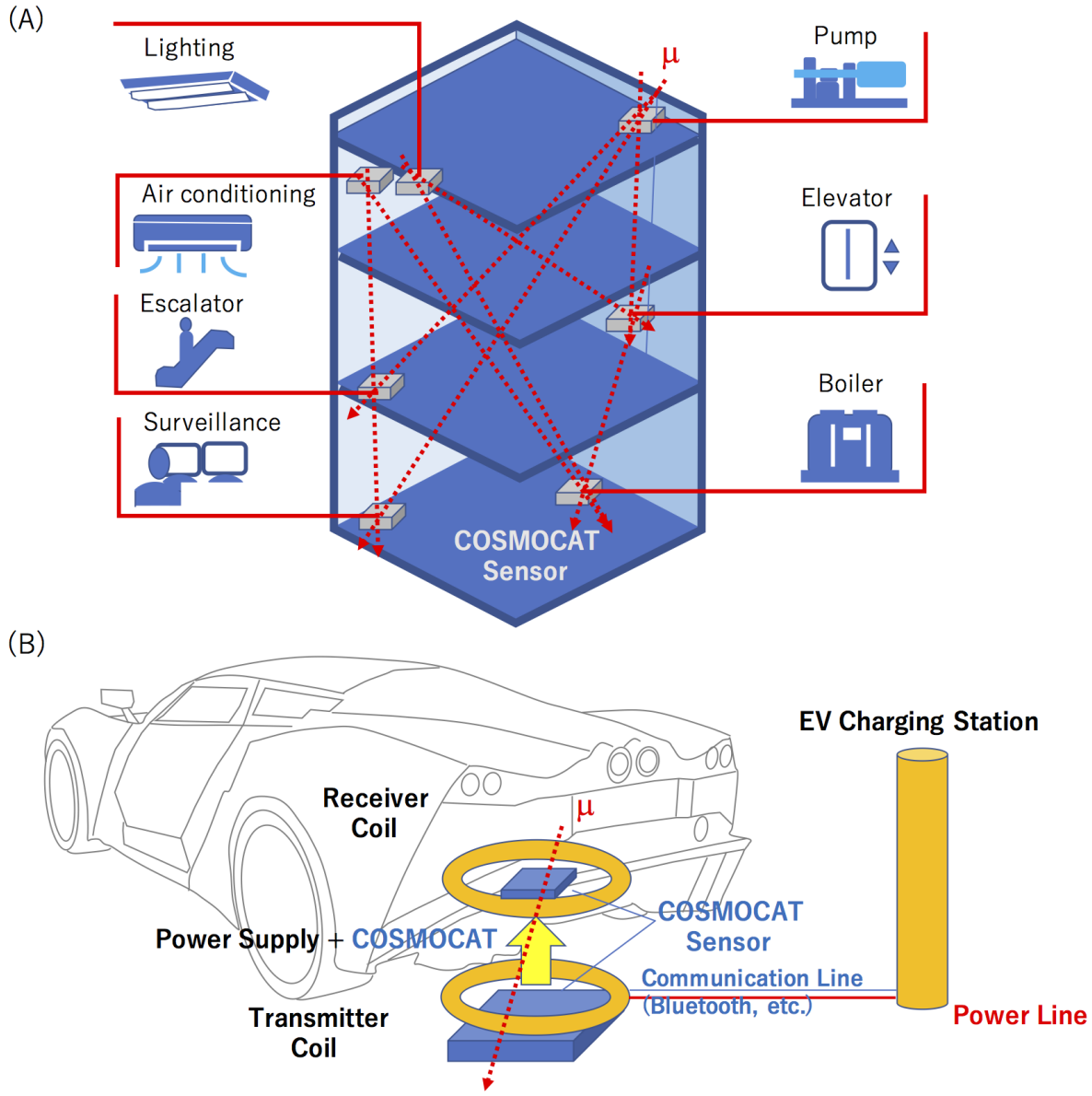

図２：COSMOCAT の応用例

（A）スマートビルディングへの活用。（B）空間伝送型ワイヤレス電力伝送システムへの活用。

図３（A）にはパケット全てを 10 桁の文字列で暗号化した際の COSMOCAT の暗号化通信速度が示されている。COSMOCAT 暗号化には宇宙線ミュー粒子の到来事象が必要である。そのため、その到来頻度が暗号化通信速度を律速するが、パケットあたりのデータ量を増やすことで通信速度を向上させることが可能である。また、図３（B）には、総当たり攻撃（注９）で暗号を解読するためにかかる時間が示されている。パケットごとに暗号化されているため、データ量が増えるほど暗号解読に時間がかかる。1 ギガバイトのデータを最新コンピュータを用いてデコードするのにかかる時間は 5 万年程度である。

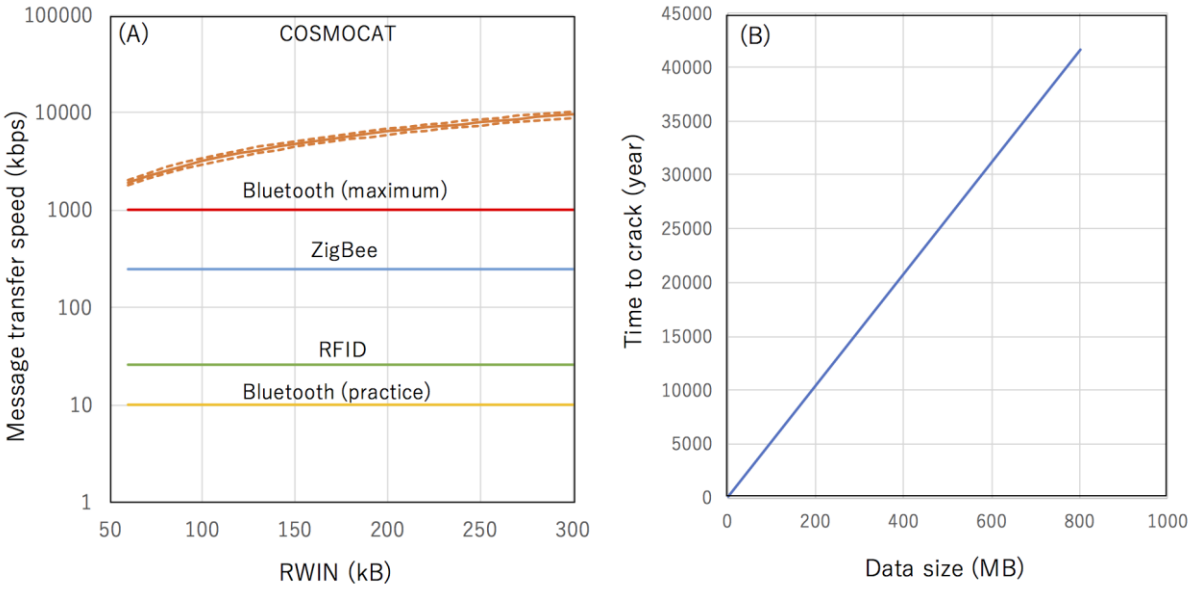

図３：COSMOCAT のパフォーマンス

（A）COSMOCAT の暗号化通信速度。（B）総当たり攻撃で暗号を解読するためにかかる時間。

＜今後の展望＞

現在暗号学分野ではポスト量子暗号学（注１０）として量子コンピュータが普及する前に強固な暗号化手法を配備することに注力している。COSMOCAT で用いられる暗号鍵は真性乱数であるため、量子コンピュータを用いても現実的な時間で暗号を解読することができない。また、送受信者間で暗号鍵の物理的なやりとりがないので、暗号鍵が盗まれることも考えにくい。次世代近距離通信における全く新しいワイヤレスセキュリティ技術としての普及が期待される。

４．問い合わせ先：

東京大学国際ミュオグラフィ連携研究機構 機構長
教授　田中宏幸（たなか ひろゆき）
〒113-0032 東京都文京区弥生 1 丁目 1−1
Email: ht"at"muographix.u-tokyo.ac.jp
ht"at"eri.u-tokyo.ac.jp
ht"at"virtual-muography-institute.org
※3 つのアドレスすべてにお送りください。
※"at"を@に変えてください。

国際ミュオグラフィ連携研究機構ウェブサイト: https://www.muographix.u-tokyo.ac.jp/

５．発表雑誌：
雑誌名：iScience
論文タイトル：Cosmic Coding and Transfer (COSMOCAT) for Ultra High Security Near-Field Communications
著者：Hiroyuki K.M. Tanaka
DOI 番号：10.1016/j.isci.2022.105897
アブストラクト URL：https://www.cell.com/iscience/fulltext/S2589-0042(22)02170-8

６．用語解説：
（注１）暗号鍵
データの暗号化や復号を行う際、計算手順に与える短い符号のこと。鍵が第三者に渡ることは、暗号文の秘匿性などが失われ、データが不正に閲覧されたり盗み出されたりするなど、深刻な脅威にさらされる恐れがある。また 暗号鍵がない限りは暗号化されたデータは復元できない。

（注２）宇宙線ミュー粒子
主に超新星などの銀河系の高エネルギーイベントによって光速まで加速される宇宙線と呼ばれる粒子が地球に到達すると、大気を構成する窒素や酸素の原子核と反応して高エネルギーの 2 次粒子生成する。その一つがミュオンと呼ばれる素粒子であり、貫通力が強い。

（注３）到着時間の極めて高い任意性
宇宙線ミュー粒子の到着時間は真性乱数（「次に何が来るのか、真にわからない」乱数）である。

（注４）飛行速度の普遍性
宇宙線ミュー粒子の飛行速度は、地球上いかなる物体中においても、その運動エネルギーが自身の質量エネルギーを超えている限り、ほぼ真空中の光速度である。

（注５）量子コンピュータ
量子力学の原理を計算に応用したコンピュータ。古典的なコンピュータで解くには複雑すぎる問題を、量子力学の法則を利用して解くコンピュータのこと。現在の暗号鍵は素因数分解の難しさで安全を担保しているため、量子コンピュータを用いることで現実的な時間で解読が可能となる。

（注６）近距離通信
Near field communication の訳語である。Bluetooth を用いた通信などに代表される。

（注７）スマートビルディング
ビル内の設備をインタラクティブに制御する仕組み。例えば、ビル全体の照明制御がスマートフォンなどの端末で可能になり、省エネが進む。また、人感センサーで部屋の入

退出を管理すれば、室内に人が不在になった段階で消灯できるようになるほか、空調設備との連動も可能となる。

（注８）ワイヤレス電力伝送システム
電気機器において、金属接点やコネクタなどを介さずに電力を伝送するシステム。電波を活用したワイヤレス充電・給電システムで、有線で接続することなく利用できることから、道路に埋め込まれた装置から電気自動車へ充電するなど幅広い用途での利用が期待されている。

（注９）総当たり攻撃
ブルートフォース攻撃の日本語訳。暗号解読や認証情報取得の手法であり、主にパスワードを不正に入手するために用いられる。具体的な手法は、理論的に考えられるパスワードのパターン全てを入力するという、最も単純な方法。

（注１０）量子暗号学
量子力学の性質を積極的に活用することによって、通信内容を秘匿することを目的とした技術を指す。いくつかの種類が考案されており、主なものとして量子鍵配送が挙げられる。