5G ネットワークを用いる CPS/IoT 向け 制御システムへの暗号化制御の適用可能性

水矢　亨，千家　雅之（企画部　経営戦略課　新事業戦略グループ）

阿部　顕一（企画部　経営戦略課）

1.　はじめに

5G は、超高速・大容量、超低遅延、多数同時接続を特長とするモバイル向けの無線通信として注目されている。製造業をはじめとする産業分野においては、低遅延を特徴とする無線通信であることに加え、一般企業や自治体等で自営できるローカル 5G の制度が設けられていることから、CPS(Cyber Physical System)/IoT への活用も期待されている。当研究所でも、2020 年度にローカル 5G の無線局免許を取得し、2021 年度から海老名本部でローカル 5G（以下、「L5G」と記す。）の通信環境を運用している[1]。

5G に限らず、デジタル技術を駆使する CPS/IoT では、データ通信は欠かせない要素技術であり、それに伴ってセキュリティ対策もまた重要である。CPS/IoT におけるセキュリティ対策は、センサーや制御対象などが実在するフィジカル空間（現実空間）に損害を与えうる重要度の高いデータを扱うこと[2]、及び端末数の増加等によりネットワークの複雑性が増すことによって通常のセキュリティ対策では満足しない可能性がある。このような懸念に対し、フィジカル空間内に制御対象がある制御システムのセキュリティ対策として暗号化制御が提案されている[3], [4]。暗号化制御では、準同型性を持つ暗号アルゴリズムを利用し、制御器での処理を暗号データのまま実行できる演算（秘密計算）に限定することで、サイバー攻撃の予防と検知に強い制御器を実現する。

本稿では、当研究所の L5G 環境を利用し、高速性や低遅延性が期待される L5G における暗号化制御の適用可能性を検討する。そのために、L5G ネットワーク上で暗号化制御の演算処理を実行し、その処理時間を測定・評価する。

2.　CPS/IoT と暗号化制御

2.1　サイバー空間とフィジカル空間

一般的に CPS/IoT は、データが集積されるサイバー空間（仮想空間）とセンサーや制御対象機器などが配置されるフィジカル空間（現実空間）の両者に跨る[2]。スマート工場など産業分野での L5G も、サイバー・フィジカル間での利用が期待されている。サイバー・フィジカル・セキュリティ・フレームワーク（CPSF）[2]では、これをふまえたセキュリティ対策の全体像が示されている。CPSF では、産業社会を 3 層構造と捉え、各層で求められる信頼性を図 1 のように示している。このうち、第 2 層がサイバー空間とフィジカル空間の相互作用が生じる部分であり、IoT や CPS に由来する部分となっている[5]。

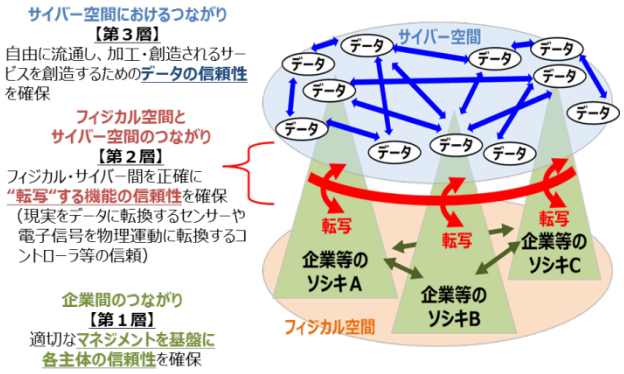

図 1　CPSF における 3 層構造と求められる信頼性[2]

2.2　ElGamal 暗号による暗号化制御

暗号化制御[3], [4]では、制御対象において入出力信号データや制御パラメータの暗号化・復号化等を行い、制御器では秘密計算処理だけになるように制御系を構成する。CPSF でいえば、サイバー空間にある制御器には暗号化された値しか提供しない暗号化制御は、第 2 層でのセキュリティ対策と捉えることができる。

この暗号化制御は準同型性をもつ暗号を用いて実現できる。暗号化の操作 Enc に対し、暗号化される前と後のデータそれぞれに対して（加減乗除のような）演算子$\bullet_P$と$\bullet_E$が定められているとき、次式が成立すれば、暗号化 Enc は演算$\bullet$ について準同型性をもつといわれる。

$$\mathrm{Enc}(m \bullet_P n) = \mathrm{Enc}(m) \bullet_E \mathrm{Enc}(n)$$

例えば、公開鍵暗号の一つである ElGamal 暗号は、乗法について準同型性をもつ。

一般的な線形制御は、時間を離散化した場合、次式のように表現される。

$$\begin{bmatrix} x(t+1) \\ u(t) \end{bmatrix} = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} x(t) \\ v(t) \end{bmatrix}$$

ここで、x は制御器の状態変数、u は制御入力、v は制御器への入力であり、A、B、C、D は制御器のパラメータである。上式が ElGamal 暗号化可能な形に量子化されている場合、乗法準同型性をもつ ElGamal 暗号の暗号化と復号化の操作を Enc と Dec とすると、次式が成立する。

$$\begin{bmatrix} Ax(t)+Bv(t) \\ Cx(t)+Dv(t) \end{bmatrix} = \begin{bmatrix} \mathrm{Dec}[\mathrm{Enc}(Ax(t))]+\mathrm{Dec}[\mathrm{Enc}(Bv(t))] \\ \mathrm{Dec}[\mathrm{Enc}(Cx(t))]+\mathrm{Dec}[\mathrm{Enc}(Dv(t))] \end{bmatrix}$$

$$= \begin{bmatrix} \mathrm{Dec}[\mathrm{Enc}(A)\,\mathrm{Enc}(x(t))]+\mathrm{Dec}[\mathrm{Enc}(B)\,\mathrm{Enc}(v(t))] \\ \mathrm{Dec}[\mathrm{Enc}(C)\,\mathrm{Enc}(x(t)]+\mathrm{Dec}[\mathrm{Enc}(D)\,\mathrm{Enc}(v(t))] \end{bmatrix}$$

ここで、最初の等号は、Enc に続いて Dec を行うと暗号化前の値が得られることによる。右辺のうち、暗号データの乗算とそれ以外（暗号化／複合化／平文の加算）の実行を制御器と制御対象に分離すれば暗号化制御が実現される。

3. 評価方法

3.1 計測方法

2.2 節で紹介した線形制御の ElGamal 暗号による暗号化制御は、ElGamal 暗号化可能な量子化が必要ではあるが、一般的なベクトルと行列の乗算

$$\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \cdots & A_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

を対象と考えることができる。ここでは、上式で n=3 の場合について、制御対象に相当する PC#1 と制御器に相当する PC#2 の 2 台の PC を L5G ネットワークに接続して、

0) PC#1 で鍵長を指定して、公開鍵と秘密鍵を生成
1) PC#1 で 3×3 行列$[A_{ij}]$の各成分を暗号化し、$[\mathrm{Enc}(A_{ij})]$を PC#2 に UDP で転送
2) PC#1 で 3 次元ベクトル$[x_i]$の各成分を暗号化し、$[\mathrm{Enc}(x_1)、\ \cdots、\ \mathrm{Enc}(x_n)]$を PC#2 に UDP で転送
3) PC#2 で、$[\mathrm{Enc}(A_{i1})\mathrm{Enc}(x_1), \cdots, \mathrm{Enc}(A_{in})\mathrm{Enc}(x_n)]$を暗号データの乗法のみで計算し、PC#1 に UDP で転送。これを、各 i(=1～n)に対して繰り返す。
4) PC#1 で、3)で転送されたベクトルの各成分を復号し、復号された各成分の和を計算する。これが $[y_i]$の各成分に対応する。

の各処理を行い、2)から 4) の処理 100 回分の時間を計測した。

3.2 システム構成

計測に用いた 2 台の PC は、いずれも CPU に Core i5-1135G7 を搭載し、メモリは 16GB である。また、そのソフトウェア構成は次のとおりである。

・OS：Ubuntu 20.04 LTS 64bit
・プログラミング言語：Python 3.8.10
（Pycryptdome 3.15.0 と Numpy 1.23.1 も利用）

なお、L5G 接続の場合に用いた L5G のシステムは図 2 のようにオンプレミスでの構成となっている。

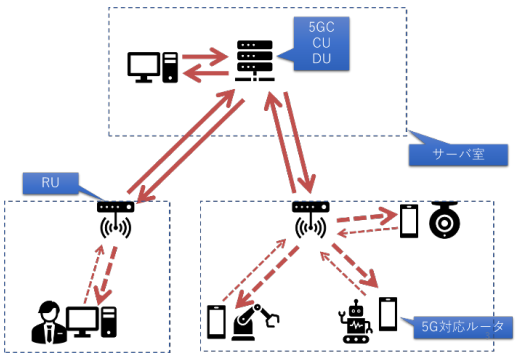

図 2 L5G の構成

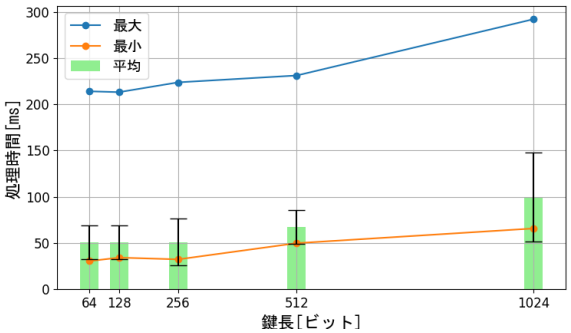

図 3 L5G での処理時間の計測結果

4. 結果及び考察

3.1 節で示した処理時間の計測を、L5G 接続下での計測結果を図 3 に示す。図中のエラーバーは標準偏差を示している。L5G 接続下では、鍵長の値にかかわらず処理時間の最大値が 200～300 ms となる結果となった。これは、暗号化制御の処理を周期的に実行させる場合、短い鍵長 64 ビットを選択したとしても、200 ms 以上の周期を設定する必要があることを意味する。また、鍵長が 64～256 ビットの範囲では、処理時間に対する鍵長の影響は小さく、暗号化制御の演算処理に比べ L5G 通信の遅延の影響が大きくなっていると考えられる。512 ビット以上の鍵長では、暗号化制御の演算処理の影響も現れていると推測される。

5. おわりに

本稿では 5G ネットワークを用いる CPS/IoT を想定し、その中で動作する制御システムへの暗号化制御の適用可能性を、当研究所の L5G を用いた処理時間の測定と評価を通じて検証した。暗号化制御の演算処理を L5G ネットワーク上で実行し、その処理時間を計測したところ、L5G の通信遅延の影響が大きいことが分かった。特に、鍵長の値にかかわらず処理時間の最大値が 200～300 ms となったことから、制御周期を考えると制御系への適用は制御周期を見ながら慎重に検討する必要があることも分かった。

【謝辞】

2021 年度の電気通信大学との共同研究において小木曽先生ならびに小木曽研究室の皆様には暗号化制御についてご指導・ご助言をいただきました。記して謝意を表します。

【参考文献】

1. 神奈川県立産業技術総合研究所：KISTEC ANNUAL REPORT 2022 (2022).
2. 経済産業省：サイバー・フィジカル・セキュリティ対策フレームワーク Version 1.0 (2019).
3. K. Kogiso and T. Fujita: ”Cyber-security enhancement of networked control systems using homomorphic encryption”, Proc. IEEE Conf. Decis. Control, pp.6836-6843 (2015).
4. 藤田, 小木曽:「ElGamal 暗号を用いた制御器の暗号化」, 計測自動制御学会論文集, Vol. 51, No.9, pp.661-666 (2015).
5. 経済産業省：IoT セキュリティ・セーフティ・フレームワーク Version 1.0 (2020).