مجله کنترل
ISSN (print) 2008-8345
ISSN (online) 2538-3752
مقاله پژوهشی
جلد۱۷، شماره ۲، تابستان ۱۴۰۲، صفحه ۱۹۴-۱۷۹

مروری بر روش‌های کنترل رمزنگاری شده برای حفظ حریم خصوصی در سیستم‌های سایبرفیزیکی

سعید عادلی پور[۱] و محمد حائری[۲]

[۱] پژوهشگر پسادکتری، دانشکده مهندسی برق، گروه کنترل، دانشگاه صنعتی شریف،تهران، ایران saeed.adelipour@gmail.com
[۲] استاد، دانشکده مهندسی برق، گروه کنترل، دانشگاه صنعتی شریف، تهران،ایران haeri@sharif.ir

دریافت: ۱۴۰۲/۰۵/۰۱ پذیرش: ۱۴۰۲/۰۶/۲۳

چکیده: بهره‌گیری از مفاهیم رایانش ابری و محاسبات توزیع‌یافته، مزایای متنوعی نظیر عملکرد بهتر، امکان برون‌سپاری محاسبات پیچیده و مقیاس‌پذیری سریع را در بسیاری از سیستم‌های کنترل شبکه‌ای مانند شبکه‌های هوشمند انرژی، ساختمان‌های هوشمند، حمل و نقل هوشمند و ... ایجاد کرده است. از طرف دیگر، خطر افشا شدن اطلاعات مهم، دست‌کاری شدن آن‌ها توسط عوامل خارجی و کاهش اعتماد عمومی به روش‌های کنترل غیرمتمرکز و توزیع‌یافته که در آن عامل‌ها ممکن است به دلایل مختلف مایل به اشتراک‌گذاری اطلاعات نباشند، از مهم‌ترین چالش‌های موجود در کنترل سیستم‌های سایبرفیزیکی است. این مقاله به مرور روش‌های کنترل رمزنگاری شده، که با حفظ حریم خصوصی به برخی از این چالش‌ها پاسخ می‌دهند، می‌پردازد. در این روش‌ها، محاسبات مورد نیاز به طور مستقیم بر روی سیگنال‌های رمزنگاری شده انجام می‌شود و نیازی به باز کردن رمز و در معرض خطر قرار دادن اطلاعات مهم وجود ندارد. این کار امکان دسترسی حمله‌کننده‌ها به اطلاعات حیاتی سیستم کنترلی را بسیار محدود می‌کند و از آن‌جایی که برای طراحی حملات پیچیده‌تر عموماً به اطلاعات به دست آمده از سیستم نیاز است، حفظ خصوصی بودن سیگنال‌ها در تمام حلقه‌ی کنترل احتمال طرح حمله‌های سایبری پیچیده‌تر را نیز به طور قابل ملاحظه‌ای کاهش می‌دهد. از این رو در این مقاله، رمزنگاری هم‌ریختی و محاسبات چندجانبه‌ای امن به عنوان پایه‌های حفظ حریم خصوصی و ایجاد روش‌های کنترلی امن معرفی شده و روش‌های کنترل و بهینه‌سازی توسعه یافته بر مبنای آن‌ها مرور می‌شوند. کاستی‌ها و چالش‌های روش‌های موجود بحث شده و مسیر آینده‌ی تحقیقات در این رویکرد نوظهور در مهندسی کنترل ترسیم می‌شود.

کلمات کلیدی: کنترل امن، کنترل رمزنگاری شده، سیستم‌های سایبرفیزیکی، حفظ حریم خصوصی، محاسبات چندجانبه امن، رمزنگاری هم‌ریختی.

A Review of Privacy Preserving Encrypted Control for Cyber-Physical Systems

Saeed Adelipour and Mohammad Haeri

Abstract: Utilizing cloud computing and distributed computing has led to various advantages like enhanced performance, enabling outsourcing of complex computations, and higher scalability in a vast range of network control systems such as smart energy networks, smart buildings, and intelligent transportation. However, confidentiality breaches and manipulation of sensitive and private information, as well as lack of public trust in cloud-based decentralized and distributed approaches where agents are reluctant to share their information due to privacy concerns are among the emerging challenges in control of cyber-physical systems. This paper reviews the privacy-preserving encrypted control methods that address some of these challenges. In encrypted control methods, all the required computations are performed directly on the encrypted data, and thus, no intermediate decryption of private data is needed.

In this way, the access of adversaries to the crucial information of the control system will be very restricted. Since implementing a complex cyberattack usually requires an in-depth knowledge of the system's data, protecting the privacy of the system's signals in the entire control loop considerably reduces the possibility of more complex cyberattacks. Therefore, in this paper, homomorphic encryption and secure multi-party computation methods are introduced as the basis for preserving the privacy of data and designing secure control approaches. Then, various control and optimization methods are reviewed. Shortcomings and challenges of existing results are discussed and the roadmap to further research in this emerging topic in control engineering is drawn.

Keywords: Secure control, Encrypted control, Cyber-physical systems, Privacy-preserving, Secure multi-party computation, Homomorphic encryption.

۱- مقدمه

با پیشرفت مفاهیم رایانش ابری[1] و محاسبات توزیع‌یافته، قسمت‌های فیزیکی و غیرفیزیکی مربوط به مخابرات، کنترل و ابزاردقیق موجود در بسیاری از سیستم‌های کنترل شبکه‌ای با یکدیگر متصل شده و مفهوم نوینی به عنوان سیستم‌های سایبرفیزیکی[2] را پدید آورده‌اند. این سیستم‌ها در بسیاری از کاربردهای مهم مربوط به زندگی روزمره مورد استفاده قرار گرفته‌اند که از جمله‌ی آن‌ها می‌توان به شبکه‌های هوشمند انرژی، ساختمان‌های هوشمند، شبکه‌های حمل و نقل هوشمند، کنترل مجموعه‌ای ربات‌ها و بهداشت و درمان هوشمند و ... اشاره کرد. به این ترتیب، فواید زیادی از جمله عملکرد بهتر، استفاده‌ی بهینه از منابع، امکان ایجاد برون‌سپاری محاسبات و خدمات و همچنین مقیاس‌پذیری سریع به دست می‌آید [1].

از طرف دیگر، کنترل در فضای ابری ایجاب می‌کند که داده‌های حساس سیستم از طریق شبکه‌های عمومی مخابره شده و در زیرساخت‌های تحت کنترل شخص ثالث پردازش شوند که اعتماد کاملی به آن‌ها وجود ندارد. از این رو، واضح است که تمام فواید سیستم‌های سایبرفیزیکی تنها در صورتی می‌توانند ارزشمند باشند که بتوان امنیت داده‌های منتقل شده در فضای ابری و خصوصی ماندن آن‌ها را تضمین کرد. عدم موفقیت در محافظت از داده‌های موجود در سیستم کنترل می‌تواند خسارت‌های جبران‌ناپذیری به کل مجموعه وارد کند [2, 3]. به عنوان نمونه‌های مهم در این زمینه می‌توان به حمله‌ی استاکس‌نت[3] به تجهیزات هسته‌ای کشور در سال ۲۰۰۹ میلادی و حمله به زیرساخت‌های شبکه برق اوکراین در سال ۲۰۱۵ اشاره کرد [3, 4].

با توجه به اهمیت زیاد امنیت در کنترل سیستم‌های شبکه‌ای و سایبرفیزیکی و از آن‌جایی که این موضوع در بسیاری از جنبه‌ها هنوز در ابتدای راه قرار دارد، مراجع مختلفی تلاش کرده‌اند تا با ارائه دسته‌بندی از انواع آسیب‌پذیری‌ها، سیاست‌های حمله و راه‌کارهای ارائه شده، نقشه‌ی راهی برای ادامه پژوهش و پیش‌برد مرز دانش در این زمینه فراهم سازند. امنیت سیستم‌های سایبرفیزیکی را می‌توان از منظر مخابرات یا تئوری اطلاعات بررسی کرد. اما از آن‌جایی که این سیستم‌ها در کنترل بسیاری از زیرساخت‌های اساسی جامعه نقش اساسی دارند، بررسی امنیت سایبری کنترل این شبکه‌ها نیز اهمیت زیادی می‌یابد. از این رو اخیرا تلاش‌هایی شده تا زوایای این موضوع از منظر مهندسی کنترل نیز مورد بررسی قرار گیرد [2-12]. مرجع [8] یک مطالعه مروری کتابخانه‌ای در مورد انواع حمله‌های سایبری از منظر مهندسی کنترل انجام داده است. حمله‌های سایبری با توجه به ماهیت خرابکاری طبقه‌بندی شده و مقالات مرتبط با هر کدام از حمله‌ها لیست شده است. امنیت سیستم‌های سایبرفیزیکی از دیدگاه سیستم‌های کنترل در [2] بررسی شده است. در این مقاله علاوه بر دسته‌بندی حمله‌ها، روش‌های برخورد با حمله‌های سایبری در سه دسته پیشگیری از وقوع حمله، تاب آوری در برابر حمله، و شناسایی و خنثی کردن حمله بررسی و مصداق‌های آن در شبکه‌های قدرت و حمل و نقل مطالعه شده‌اند.

برخی از مقالات مروری تمرکز خود را بر روی سیستم سایبرفیزیکی با کاربرد خاص یا یک روش کنترلی مشخص قرار داده‌اند تا بتوانند مقالات با وحدت موضوعی بیشتری را پوشش دهند. مرجع [9] با تمرکز بر موضوع ساختمان‌های هوشمند و سیستم اتوماسیون ساختمانی، حمله‌های ممکن به این دسته از سیستم‌ها را بررسی کرده و راه‌های شناسایی حمله‌ها و کاهش اثر آن‌ها را معرفی کرده است. مرجع [10] امنیت سایبری در ساختارهای کنترل پیش‌بین توزیع یافته را بررسی کرده است. خصوصی ماندن اطلاعات و امنیت روش‌های یادگیری مشارکتی در [11] مورد بررسی قرار گرفته است. در میان مراجع فارسی، نویسندگان [12] یک مطالعه مروری بر امنیت سایبری در سیستم‌های کنترل صنعتی انجام داده‌اند. در این مقاله به لزوم بررسی امنیت سایبری در سیستم‌های اتوماسیون صنعتی فرای رهیافت‌های امنیت فناوری اطلاعات اشاره شده و سپس مقالات مربوط به انواع آسیب‌پذیری‌های سیستم‌های کنترل صنعتی در سطوح مختلف و برخی حمله‌های امکان‌پذیر با تمرکز بر راه‌کارهای شناسایی حمله‌های اتفاق افتاده و کاهش اثرات آن‌ها مرور شده‌اند.

با توجه به موارد فوق، مقاله حاضر به مرور و بررسی پژوهش‌های مرتبط با طراحی و اجرای روش‌های کنترلی رمزنگاری شده به منظور حفظ حریم خصوصی در سیستم‌های سایبرفیزیکی می‌پردازد. منظور از روش

[1] Cloud computing
[2] Cyber-physical systems
[3] Stuxnet

کنترلی رمزنگاری شده، روشی است که در آن برای انتقال سیگنال‌ها از لایه‌ی فیزیکی به لایه سایبری و بالعکس و همچنین برای محاسبه‌ی قانون کنترل – که در لایه‌ی سایبری یک سیستم سایبرفیزیکی انجام می‌شود – از سیگنال‌های رمزنگاری[1] شده استفاده شود و نیازی به باز کردن رمز در هیچ مرحله‌ای نباشد. در واقع تمام محاسبات مورد نیاز برای به دست آوردن قانون کنترل به طور مستقیم بر روی سیگنال‌های رمزنگاری شده انجام می‌شود و مقدار واقعی سیگنال برای واحد محاسبه‌گر مشخص نخواهد شد. به این ترتیب، خصوصی بودن داده‌های حساس در تمام حلقه‌ی کنترل حفظ شده و از افشا شدن آن برای عامل خرابکار خارجی جلوگیری خواهد شد. برخلاف روش معمول که در آن سیگنال‌ها تنها در کانال‌های مخابراتی و در هنگام انتقال به کنترل‌کننده‌ی مستقر در فضای ابری در حالت رمزشده قرار دارند و برای انجام محاسبات از حالت رمزشده خارج می‌شوند، در کنترل رمزنگاری شده آسیب‌پذیری سیستم سایبرفیزیکی در مقابل حملات استراق‌سمع[2] و به طبع آن سایر حملات پیچیده‌تر به میزان قابل توجهی کاهش می‌یابد.

علاوه بر موارد فوق، اهمیت حفظ خصوصی بودن داده‌ها در سیستم‌های کنترلی، ایجاد اعتماد عمومی به روش‌های کنترل غیرمتمرکز و توزیع‌یافته و گسترش دایره‌ی کاربرد این روش‌ها است [16-13]. به عنوان مثال می‌توان به روش‌های بهینه‌سازی توزیع‌یافته برای بهبود توان مصرفی شبکه یا کنترل ترافیک اشاره کرد که در آن لازم است خودروهای الکتریکی داده‌های خصوصی خود نظیر میزان شارژ مصرفی یا مبدا و مقصد را با دیگر خودروها یا کنترل‌کننده‌ی مستقر در فضای ابری به اشتراک بگذارند. به طور معمول، افراد و عامل‌ها به دلایل مختلف مانند ترس از جریمه یا ترس از سوء استفاده رقیبان از اطلاعات آن‌ها و ... مایل به این کار نیستند. بنابراین، طراحی کنترل‌کننده‌ها و روش‌های بهینه‌سازی که خصوصی بودن داده‌ها در تمام مراحل (نه فقط در هنگام مبادله) حفظ شود می‌تواند از عدم اعتماد افراد به این روش‌ها کاسته و اجرای آن‌ها را موفق‌تر نماید.

اهمیت دیگر روش‌های کنترلی که تمام محاسبات را بر روی داده‌های رمزنگاری شده انجام می‌دهند، امکان ایجاد رهیافت‌های برون‌سپاری محاسبات و توسعه مفهوم «کنترل به عنوان یک خدمت[3]» است که در آن به عنوان مثال، یک شرکت می‌تواند بدون نگرانی از افشای اطلاعات، بار محاسباتی بالای روش‌های کنترلی مورد نیاز خود مانند کنترل مدل پیش‌بین را به یک شرکت متخصص در زمینه‌ی کنترل بسپارد و به این ترتیب از ایجاد هزینه‌های اضافی جلوگیری کند [18, 17]. توجه کنید که در این موارد، تنها مبارزه با عامل خرابکار مد نظر نبوده و جلوگیری از افشای اطلاعات برای عامل‌های «درست‌کار اما کنجکاو[4]» نیز اهمیت می‌یابد. زیرا به این ترتیب، شرکت ارائه دهنده‌ی خدمت محاسبه‌ی سیگنال کنترلی، لازم نیست هیچ اطلاعات غیر رمز شده‌ای دریافت کند و محرمانه بودن اطلاعات در تمام مراحل انتقال و محاسبه‌ی سیگنال کنترلی حفظ خواهد شد. مرجع [18] با یک نگاه آموزشی مقدمه‌ای بر روش‌های کنترل رمزنگاری شده ارائه کرده، مفاهیم و ابزارهای لازم را برشمرده و در یک روند یکپارچه نحوه‌ی اجرای چند نمونه اولیه از روش‌های کنترل رمزنگاری شده را تشریح کرده است. در مقاله حاضر، علاوه بر ارائه چشم‌انداز کلی امنیت سیستم‌های سایبرفیزیکی، مرور جامع‌تری بر پژوهش‌های اخیر در حوزه‌ی کنترل رمزنگاری شده انجام شده است.

مطالب این مقاله در پنج بخش تنظیم شده‌اند. در بخش اول به اهمیت بررسی کنترل امن و خصوصی ماندن اطلاعات در سیستم‌های سایبرفیزیکی پرداخته شد. گستردگی مطالب و برخی تلاش‌ها برای دسته‌بندی کارهای انجام شده و جهت‌دهی به پژوهش‌های جدید در این زمینه بیان شد. بخش دوم به مفهوم کلی امنیت سیستم‌های سایبرفیزیکی می‌پردازد. در این بخش ابتدا اهداف امنیت در سیستم‌های سایبرفیزیکی بیان شده و مطابق با آن انواع حمله‌هایی که این اهداف را نقض می‌کنند ارائه می‌شوند. بخش سوم به روش‌های مبتنی بر رمزنگاری برای حفظ حریم خصوصی اختصاص دارد. مفهوم کنترل رمزنگاری شده ارائه شده و روش‌های رمزنگاری که قابلیت به‌کارگیری در روش‌های کنترلی را دارند مرور می‌شوند. در این بخش سعی شده تا عموم روش‌های کنترل و بهینه‌سازی رمزنگاری شده که تاکنون وجود دارند، معرفی شوند. در بخش چهارم، برخی از چالش‌های اساسی پیش رو در بحث کنترل رمزنگاری شده معرفی شده و مسیرهای پژوهشی باز که نیاز به بررسی بیشتری دارند به طور خلاصه ارائه می‌شود. در نهایت، بخش پنجم به جمع‌بندی مطالب می‌پردازد.

۲- امنیت سیستم‌های سایبر فیزیکی

همانطور که گفته شد، هر چه اجزای بیشتری از سیستم سایبرفیزیکی به شبکه متصل باشد، عملکرد آن به طور بالقوه تحت الشعاع حملات سایبری بیشتری قرار می‌گیرد. برای طراحی یک روش کنترلی امن، ابتدا لازم است تا چگونگی خطرات سایبری و میزان توانایی‌های عامل‌های خراب‌کار به درستی مشخص شود. در واقع آنچه حمله‌های سایبری را از خطاهای معمول سیستم‌های سایبرفیزیکی متمایز می‌کند، هدفمند بودن حمله و استفاده‌ی حمله‌کننده از اطلاعاتی است که از سیستم در اختیار دارد. بنابراین نیاز است تا با درک درست از اهداف و توانایی‌های حمله‌کننده، مدلی از حمله به دست آورد و مطابق با آن چاره‌جویی کرد [5].

۲-۱. اهداف امنیت در سیستم‌های سایبرفیزیکی

اهداف امنیتی در سیستم‌های سایبرفیزیکی را می‌توان بر اساس آنچه در امنیت سیستم‌های فناوری اطلاعات مرسوم بود تعریف کرد. به طور کلی، در جهت حفظ امنیت در سیستم‌های کنترلی نیاز است تا سه هدف خصوصی ماندن[5]، صحیح ماندن[6] و در دسترس ماندن[7] اطلاعات برآورده شوند تا عملکرد صحیح سیستم برقرار باشد [3, 5, 8]. مصداق این اهداف در یک سیستم سایبرفیزیکی را می‌توان به صورت زیر نوشت.

خصوصی ماندن: نیاز است تا از محرمانه بودن اطلاعات مهم و حساس سیستم در مقابل عامل‌های غیرمجاز محافظت شده و از افشای

[1] Encrypted signals
[2] Eavesdropping attacks
[3] Control as a service
[4] Honest but curious
[5] Confidentiality
[6] Integrity
[7] Availability

غیرضروری داده‌ها جلوگیری شود. در سیستم‌های کنترلی مانیتورینگ داده‌های حساس و در معرض قرار گرفتن پارامترهای سیستم و کنترل‌کننده و سیگنال‌های میانی برای عامل‌های خارجی چه در هنگام مخابره میان اجزای سیستم و چه در هنگام پردازش در واحدهای محاسبه‌گر ممکن است این هدف را دچار مخاطره کند.

صحیح ماندن: لازم است تا از مقدار صحیح و درست داده‌ها در تمام اجزای سیستم کنترل استفاده شود. در یک سیستم کنترلی داده‌های سنسور قبل از انتقال به کنترل‌کننده ممکن است دستکاری شده یا به کلی تغییر یابند. همچنین، پارامترهای کنترل‌کننده ممکن است طوری دستکاری شوند تا پاسخ به دست آمده از روش کنترلی با پاسخ صحیح مورد نظر متفاوت شده و عملکرد سیستم مختل شود.

در دسترس ماندن: داده‌ها باید همواره در زمان مناسب در دسترس اجزای سیستم قرار بگیرند. بنابراین باید از تاخیر میان سیگنال‌های اندازه‌گیری شده با واحد محاسبه‌گر، ایجاد شدن تاخیر محاسباتی ناشی از مختل کردن روند اجرای الگوریتم‌های کنترلی یا به کلی قطع کردن ارتباط میان اجزا مانند نرسیدن سیگنال کنترلی محاسبه شده به عملگرهای سیستم جلوگیری شود.

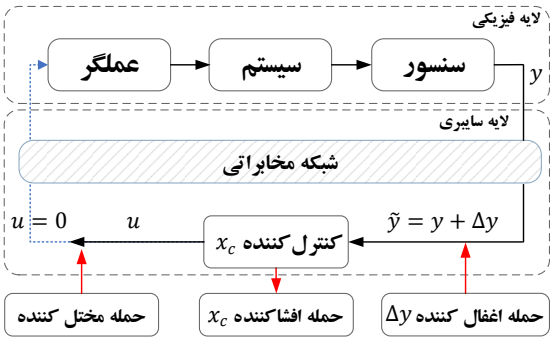
۲-۲. انواع حمله‌های سایبری

از منظر عامل خرابکار، به خطر انداختن هر کدام از اهداف امنیتی گفته شده در بخش قبل را می‌توان به ترتیب به صورت حمله‌های افشاکننده[1]، حمله‌های اغفال‌کننده[2] و حمله‌های مختل‌کننده[3] دسته‌بندی کرد [2-5, 8].

حمله‌های افشاکننده: به تمام مواردی گفته می‌شود که باعث افشا شدن اطلاعات سیستم می‌شود و هدف خصوصی ماندن اطلاعات سیستم را تهدید می‌کنند که از جمله‌ی آن‌ها می‌توان به استراق سمع اشاره کرد. هدف عامل خرابکار می‌تواند استفاده مستقیم از اطلاعات به دست آمده از این حمله باشد (مانند فروش اطلاعات حساس به رقیب تجاری) یا از آن برای ایجاد دسترسی بیشتر در سیستم یا پی بردن به سایر اطلاعات سیستم نظیر تابع تبدیل سیستم یا کنترل‌کننده استفاده کند که به آن حمله استنتاج[4] گفته می‌شود.

حمله‌های اغفال‌کننده: در این دسته از حمله‌ها مقادیر سیگنال‌ها دچار تغییر و دستکاری شده و هدف صحیح بودن و قابل اعتماد بودن داده‌ها برای اجزای سیستم کنترلی از دست می‌رود. به عنوان مثال، حمله‌ی تزریق داده‌ی غلط[5] که در آن خرابکار یک داده‌ی گمراه‌کننده را به داده‌ی اصلی اندازه‌گیری شده توسط سنسور یا به سیگنال کنترلی محاسبه شده قبل از رسیدن به عملگر اضافه می‌کند.

حمله‌های مختل‌کننده: در این حمله‌ها سیگنال به کلی مسدود شده یا طوری دچار تاخیر می‌شود که عملیاتی بودن آن از دست رفته و هدف در دسترس بودن آن برای اجزای سیستم در زمان مورد نظر از بین می‌رود. یک مثال در این زمینه، حمله‌ی عدم سرویس‌دهی[6] است. شکل ۱. نمونه‌ای از هرکدام از این حمله‌ها و یک محل احتمالی اعمال آن حمله که در اصطلاح به آن سطح حمله[7] گفته می‌شود را در ساختار کنترل سیستم‌های سایبرفیزیکی نشان می‌دهد.



شکل ۱. نمونه‌ای از حمله‌های افشاکننده، اغفال‌کننده و مختل‌کننده و محل احتمالی اعمال حمله در ساختار سیستم سایبرفیزیکی.

از یک منظر دیگر حمله‌ها را می‌توان به دو نوع غیر فعال (بدون دخالت مستقیم در داده‌های سیستم) و فعال (با ایجاد تاثیر مستقیم بر سیگنال‌های سیستم) تقسیم کرد. حمله‌های غیرفعال مانند حمله‌ی استراق سمع هر چند ساده‌تر به نظر می‌رسند اما تشخیص این‌گونه حمله‌ها دشوارتر است. همچنین، در طی این حمله‌ها بدون آنکه واحدهای تشخیص ناهنجاری[8] در سیستم بتوانند وجود عامل خرابکار را تشخیص دهند، تمام اطلاعات مهم و حیاتی سیستم ممکن است به سرقت رفته و دانش لازم برای اجرای یک حمله‌ی فعال پیچیده توسط خرابکار کسب شود.

البته این دسته‌بندی تمام حمله‌ها را به طور مجزا توصیف نمی‌کند و در عمل حمله‌های موفق عموماً ترکیبی از این موارد هستند. به عنوان یک نمونه مهم از حملات ترکیبی که در آن از خصوصی نبودن داده‌ها در تمام حلقه‌ی کنترل سوء استفاده شده است، می‌توان به حمله‌ی استاکس‌نت به تجهیزات غنی‌سازی اورانیم کشور در سال ۲۰۰۹ میلادی اشاره کرد. در این حمله، ابتدا بدافزار مورد نظر وارد سیستم شده و برای مدت طولانی بدون شناسایی شدن، اقدام به مشاهده و ضبط اطلاعات حیاتی و مهم سیستم کرد. به این ترتیب، توانست خروجی‌های مهم سیستم را در هنگام عملیات درست و پایدار مشاهده کرده و آن‌ها را برای واحد مانیتورینگ تکرار کند. سپس، سیگنال‌های غلط مخرب را به عملگرهای سیستم ارسال کرد در حالی که واحد مانیتورینگ همان سیگنال‌های به ظاهر سالم را مشاهده می‌کرد و نتوانست وقوع حمله را تشخیص دهد. این حمله که از جنس حمله‌ی تکرار[9] است را می‌توان ترکیبی از حمله‌ی افشاکننده و اغفال‌کننده دانست و اهمیت خصوصی ماندن تمام سیگنال‌های کنترلی در کل حلقه‌ی کنترل را نشان می‌دهد [2, 8].

به عنوان مثال دوم می‌توان به حمله به شبکه برق اوکراین در سال ۲۰۱۵

[1] Disclosure attacks
[2] Deception attacks
[3] Disruption attacks
[4] Inference attack
[5] False data injection
[6] Denial of service
[7] Attack surface
[8] Anomaly detector
[9] Replay attack

میلادی اشاره کرد. در این مورد، حمله‌کننده ابتدا از طریق ایمیل‌های مخرب وارد سیستم شد و توانست به بخشی از اطلاعات مهم دسترسی داشته باشد. سپس از این اطلاعات برای دسترسی به قسمت‌های حیاتی‌تر استفاده کرده و با طراحی یک حمله‌ی جعل[1]، فرمان‌های کنترلی مخرب را در شبکه اعمال کند. در این مورد نیز از دست رفتن خصوصی بودن اطلاعات شبکه‌ی کنترلی منجر به ایجاد امکان طراحی یک حمله‌ی بزرگ‌تر شد [2, 8].

۲-۳. راه‌کارهای برخورد با حمله‌های سایبری

روش‌های برخورد با حمله‌های سایبری را می‌توان در بخش‌های پیش‌گیری، تشخیص وقوع حمله و جبران اثر آن (یا افزایش تاب‌آوری سیستم) بررسی کرد.

در گام **پیش‌گیری**، نیاز است تا با حفظ حریم خصوصی داده‌ها در سیستم، از ایجاد حمله جلوگیری کرد یا احتمال وقوع آن را کاهش داد. راه‌کار اول، استفاده از رمزنگاری برای حفظ محرمانگی داده‌ها در حلقه‌ی کنترل است. استفاده از رمزنگاری می‌تواند تنها در سطح کانال‌های مخابراتی و انتقال اطلاعات میان اجزای سیستم انجام شود [19, 20]. البته در این صورت ممکن است داده‌ها در هنگام پردازش در کنترل‌کننده توسط عوامل خارجی یا کنترل‌کننده‌ی غیرقابل اعتماد مورد حمله قرار بگیرند. بنابراین لازم است تا روش‌های رمزنگاری‌ای مورد استفاده قرار گیرند که بتوان محاسبات ریاضی را به طور مستقیم بر روی آن‌ها انجام داد [18, 21]. راه‌کار دیگر، ایجاد سطحی از ناشفافی[2] و نامعینی خودساخته در ساختار سیستم کنترل است به طوری که عامل خرابکار گمراه شده و نتواند مقدار واقعی سیگنال‌ها را دریابد [17, 22-25]. مرجع [17] با الهام از تبدیل مسائل بهینه‌سازی به مسائل معادل، روش‌هایی مبتنی بر تبدیل جبری ارائه کرده که در آن مسئله‌ی کنترلی اصلی به یک مسئله‌ی دیگر تبدیل می‌شود به طوری که عامل خرابکار نتواند با مشاهده سیگنال‌های مخابره شده میان فضای ابری و سیستم به ماهیت سیگنال‌های اصلی پی ببرد. از مزایای چنین روش‌های نسبت به روش‌های رمزنگاری بار محاسباتی بالاسری بسیار کمتر آنها است. اما از طرف دیگر، کاربرد برخی از این روش‌ها به سیستم‌ها و شرایط خاص محدود است و ممکن است جامعیت نداشته باشد.

یکی دیگر از روش‌های حفظ حریم خصوصی که در مراجع مختلفی به آن پرداخته شده، خصوصی‌ماندن تفاضلی[3] است که در آن داده‌های سیستم با یک سیگنال نویز مناسب با واریانس مشخص جمع می‌شوند تا عامل خرابکار نتواند تخمینی از داده‌های اصلی به دست آورد [26-28]. مشکل اساسی این روش‌ها از دست رفتن کیفیت پاسخ سیستم به واسطه‌ی تجمیع نویزهای اضافه شده به داده‌های موجود است به طوری که حتی امکان از دست رفتن کامل سیگنال اصلی وجود دارد. همچنین، افزودن نویز به سیگنال‌ها باعث دشوار شدن ایجاد روش‌های تشخیص خطا در سیستم می‌شود. در واقع محرمانگی در مقابل امنیت قرار می‌گیرد [29, 30].

بسیاری از سیستم‌ها سایبرفیزیکی موجود بدون در نظر گرفتن مباحث امنیتی طراحی و اجرا شده‌اند. به عنوان مثال، وجود یک صفر ناوردای[4] ناپایدار در تابع تبدیل یک فرآیند، آن را نسبت به دسته‌ای از حمله‌های غیرقابل تشخیص[5] به نام حمله دینامیک صفر[6] در معرض خطر قرار می‌دهد. زیرا صفر ناپایدار باعث می‌شود نا برخی از روش‌های تشخیص ناهنجاری در سیستم نتوانند خروجی حاصل شده را از خروجی بدون حمله سیستم تشخیص دهند. در حالی که شاید بتوان با تغییر مکان سنسورها یا تخصیص سنسورها و عملگرهای جدید از بروز این دینامیک صفر در سیستم جلوگیری کرد. بنابراین، گام دیگری در پیش‌گیری از حمله‌های سایبری، بررسی نقاط ضعف سیستم‌های موجود به منظور کاهش احتمال در معرض حمله قرار گرفتن است [31, 32].

تشخیص حمله و کاهش اثر آن در سیستم‌ها سایبرفیزیکی شامل مجموعه‌ی متنوعی از روش‌هایی است که با پایش مستمر وضعیت سیگنال‌های مهم در داخل حلقه‌ی کنترل، بروز ناهنجاری‌ها را تشخیص داده و یک سیگنال هشدار را ایجاد و مکانیزم دفاعی مرتبط را فعال می‌کنند. برخی از این روش‌ها بر اساس دانستن مدل قطعی یا تصادفی از ساختار سیستم و استفاده از رویت‌گر مناسب برای تخمین حالت‌های سیستم و مقایسه حالت‌های سیستم در حالت بدون حمله و حالت حمله بنا شده‌اند. روش‌های دیگری نیز نظیر استفاده از نهان‌نگاری[7] برای پیگیری صحت داده‌ها در حلقه‌ی کنترل یا استفاده از روش‌های مبتنی بر داده و یادگیری ماشین[8] برای تشخیص موارد ناهنجاری احتمالی پیشنهاد شده‌اند [2, 31, 33]. راهکار دیگر اتخاذ روش‌های کنترل مقاوم برای افزایش تاب‌آوری سیستم در مقابل حمله‌های احتمالی است [34]. دسته‌بندی و بررسی دقیق روش‌های تشخیص حمله و برخورد با آن‌ها که گستره وسیعی از پژوهش‌ها را شامل می‌شود خارج از توان این مقاله است و خواننده مشتاق می‌تواند به مطالعات مروری جدید مربوط به آن مراجعه کند [35-37].

۳- حفظ حریم خصوصی با کنترل رمزنگاری شده

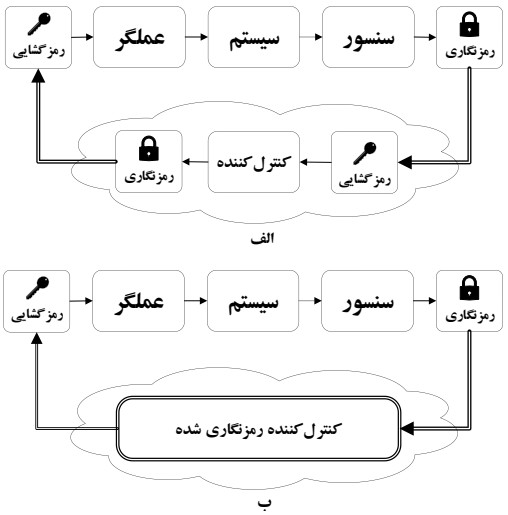
به منظور خصوصی ماندن اطلاعات موجود در حالت‌های سیستم، سیگنال کنترلی، پارامترهای کنترل‌کننده و به طور کلی داده‌های حساس سیستم در تمام اجزای حلقه‌ی کنترل، استفاده از رمزنگاری به عنوان یک راه‌کار پیشنهاد می‌شود. اعمال رمزنگاری بر داده‌های سیستم با جلوگیری از افشا شدن داده‌ها برای عامل‌های خرابکار یا کنجکاو، یک عامل پیش‌گیرانه نسبت به حمله‌های سایبری است و سطح امنیت سیستم را بهبود می‌بخشد.

۳-۱. مفهوم کنترل رمزنگاری شده

کنترل رمزنگاری شده ساختار متفاوتی با روش معمول استفاده از کانال‌های مخابراتی امن در سیستم‌های کنترل شبکه‌ای دارد. در روش معمول، داده‌ها (مثلاً مقادیر حالت‌های یک زیرسیستم) توسط کانال‌های

[1] Spoofing attack
[2] Opacity
[3] Differential Privacy
[4] Invariant zero
[5] Stealthy attack
[6] Zero-dynamic attack
[7] Watermarking
[8] Machine learning

امن بین اجزای حلقه‌ی کنترل (سایر زیرسیستم‌های شبکه یا کنترل‌کننده‌ی مستقر در فضای ابری) انتقال می‌یابند. این داده‌ها بعد از رسیدن به هر جزء، رمزگشایی شده و پس از انجام محاسبات لازم بر روی سیگنال رمزگشایی شده، دوباره برای انتقال به جزء بعدی، رمزنگاری می‌شوند و از طریق کانال‌های امن انتقال می‌یابند. این روش می‌تواند تا حدودی خصوصی بودن داده‌ها را در مقابل حمله‌کننده‌ی خارجی حفظ کند. اما در این روش، کنترل‌کننده و سایر زیرسیستم‌ها به اصل اطلاعاتی که از طریق کانال‌های محافظت شده به دست آن‌ها رسیده است، دسترسی دارند و به این ترتیب خصوصی بودن داده‌های مهم هر زیرسیستم به طور جدی در خطر قرار می‌گیرد. در مقابل، در کنترل رمزنگاری شده، داده‌های رمزشده بدون رمزگشایی و به طور مستقیم در محاسبات کنترل‌کننده مورد استفاده قرار می‌گیرند و خصوصی بودن داده‌ها در تمام حلقه‌ی کنترل حفظ شده و مقدار داده‌ها افشا نمی‌شود [18]. شکل ۲ یک کنترل‌کننده مستقر در فضای ابری را در دو حالت استفاده از کانال‌های مخابراتی رمزنگاری شده و کنترل رمزنگاری شده نشان می‌دهد. تفاوت اساسی این دو روش، عدم نیاز به رمزگشایی از داده‌ها برای انجام محاسبات لازم کنترلی است که باعث خصوصی ماندن اطلاعات در تمام حلقه‌ی کنترل می‌شود.



شکل ۲. کنترل‌کننده مستقر در فضای ابری با کانال‌های مخابراتی امن (الف) در مقایسه با روش کنترل رمزنگاری شده (ب).

با توجه به مطالب بخش قبل، اولین گام در برقراری امنیت در سیستم‌های سایبرفیزیکی پاسخ به این پرسش است که «امنیت در برابر چه چیزی باید حفظ شود؟». پاسخ به این پرسش یک مدل از توانایی‌های عوامل خرابکار، قدرت محاسباتی و بودجه آن‌ها، میزان و نوع دسترسی آن‌ها به اطلاعات سیستم و هدف آن‌ها از اجرای حمله به دست خواهد داد [3, 5, 18].

در عموم روش‌های کنترل رمزنگاری شده، مدل «درست‌کار اما کنجکاو» برای تمام واحدهای محاسبه‌گر فرض شده است. بنابراین، تمام واحدهای محاسبه‌گر پروتکل‌های محاسباتی را به درستی و بدون ایجاد خرابکاری فعالانه انجام می‌دهند، اما می‌توانند تمام داده‌هایی که به دست می‌آورند را ذخیره کرده و از تجمیع آن‌ها برای پی بردن به مقدار واقعی داده‌های حساس استفاده کنند. همچنین، عامل‌های خرابکار خارجی به صورت عامل‌های استراق سمع فرض شده‌اند که قصد دارند با انجام یک حمله غیرفعال، داده‌های سیستم را استخراج کنند که ممکن است از آن برای طراحی حمله‌های پیچیده‌تر استفاده کنند، اما در این مرحله به صحت داده‌ها حمله‌ای وارد نمی‌کنند. این مدل که در بسیاری از مراجع استفاده شده است، می‌تواند بخش بزرگی از موقعیت‌های واقعی را پوشش دهد. در این موقعیت‌ها، واحدهای محاسبه‌گر که سرورهای مستقر در فضای ابری هستند، بنابر پیروی از قوانین یا ترس از دست دادن اعتبار خود تمایلی به سرپیچی از روندها و پروتکل‌ها ندارند، اما دریافت و ذخیره‌ی داده‌های حساس مشتریان ممکن است برای آن‌ها در کاربردهای دیگر سودمند باشد [18].

۳-۲. روش‌های رمزنگاری و خاصیت هم‌ریختی

از آنجایی که در کنترل رمزنگاری شده نیاز است تا محاسبات ریاضی بر روی داده‌های رمز شده انجام شود، روش رمزنگاری اعمال شده باید دارای قابلیت خاصی باشد که صحت عملیات ریاضی انجام شده بر روی داده‌ی رمزشده حفظ شود. رمزنگاری هم‌ریختی[1] به دسته‌ای از روش‌های رمزنگاری گفته می‌شود که در آن‌ها امکان انجام محاسبات ریاضی به طور مستقیم بر روی داده‌ی رمز شده وجود دارد. به عبارت دیگر، انجام عمل ریاضی مورد نظر بر روی داده‌های رمز شده و داده‌های رمز نشده در نهایت منجر به نتیجه‌ی یکسانی خواهد شد [18, 38]. فرض کنید، s_1 و s_2 دو عدد دلخواه باشند. اگر عمل رمزنگاری را با $\mathrm{Enc}(.)$ و عمل بازگشایی رمز را با $\mathrm{Dec}(.)$ نشان دهیم، در این صورت دو شرط زیر برای عمل جمع ($\oplus$) و ضرب ($\otimes$) در یک روش رمزنگاری هم‌ریختی کامل برقرار خواهد بود.

$$s_1 s_2 = \mathrm{Dec}(\mathrm{Enc}(s_1) \otimes \mathrm{Enc}(s_2)) \qquad (۱)$$

$$s_1 + s_2 = \mathrm{Dec}(\mathrm{Enc}(s_1) \oplus \mathrm{Enc}(s_2)) \qquad (۲)$$

برای برخی از روش‌های رمزنگاری تنها رابطه‌ی (۱) برقرار است که به آن‌ها روش‌های هم‌ریختی ضربی گفته می‌شود. در مقابل، در روش‌های رمزنگاری جمعی تنها امکان برقراری رابطه‌ی (۲) وجود دارد. رمزنگاری الجمال[2] یک هم‌ریختی ضربی و رمزنگاری پیلیر[3] یک هم‌ریختی جمعی است. یعنی در روش رمزنگاری الجمال تنها عملیات ضرب و در روش رمزنگاری پیلیر تنها عملیات جمع بر روی داده‌های رمزشده مجاز است. به این روش‌ها هم‌ریختی پاره‌ای نیز گفته می‌شود، زیرا تمام عملیات‌های اصلی را پوشش نمی‌دهند [40 ,39]. علاوه بر این موارد، روش‌های رمزنگاری هم‌ریختی متنوعی در ادبیات سیستم‌های رمزنگاری وجود دارد – به عنوان مثال روش رمزنگاری هم‌ریختی جمعی جوی‌لیبرت[4]– که در نحوه‌ی اجرا و پس‌زمینه و دلیل ریاضی امنیتی که ایجاد می‌کنند با یکدیگر متفاوت هستند.

مجاز بودن تنها بخشی از عملیات ریاضی چالش زیادی برای به کارگیری رمزنگاری‌های هم‌ریختی پاره‌ای در کاربردهای پیچیده‌تر ایجاد می‌کند. از طرف دیگر، هرچند روش‌های هم‌ریختی کامل قابلیت‌های

[1] Homomorphic
[2] ElGamal
[3] Paillier
[4] Joye-Libert

ریاضیاتی بهتری ارائه می‌دهند، اما عموماً بسیار پیچیده بوده و بار محاسباتی بالایی دارند که استفاده از آن‌ها در کاربردهای کنترلی را دشوار می‌کند [21, 41]. تلاش‌هایی برای به دست آوردن خاصیت هم‌ریختی کامل با بار محاسباتی کمتر نیز انجام شده است که منجر به ارائه‌ی دسته‌ای دیگری از روش‌های رمزنگاری هم‌ریختی شده است که به آن‌ها تاحدودی هم‌ریخت کامل[1] یا هم‌ریختی اهرم شده[2] گفته می‌شود. در این روش‌های رمزنگاری، علاوه بر عمل جمع، می‌توان تعداد محدودی عمل ضرب را نیز انجام داد [42, 43]. به منظور حذف محدودیت تعداد عملیات ضرب قابل انجام و جلوگیری از بیش از حد بزرگ شدن حالت رمزشده‌ی داده و سرریزشدن نسبت به فضای پیام، روندهای بازنشانی[3] فضای داده‌ی رمزنگاری پیشنهاد شده است که بدون نیاز به داشتن کلید خصوصی رمزنگاری، امکان به روزرسانی داده‌ی رمزشده بدون بزرگ شدن ابعاد فضای پیام[4] را فرآهم می‌سازد [21, 44]. البته اجرای این روش‌های بازنشانی بار محاسباتی روش را افزایش می‌دهد. از این‌رو، همچنان در بیشتر کارهای موجود در زمینه کنترل رمزنگاری شده از روش‌های هم‌ریختی پاره‌ای ضربی یا جمعی استفاده شده است [18].

در صورتی که چندین واحد محاسبه‌گر (سرور) در ساختار کنترل وجود داشته باشد، یک راه‌کار دیگر برای حفظ خصوصی ماندن داده‌ها، روش رمزنگاری اشتراک‌گذاری راز[5] است که در آن داده‌ی مورد نظر (راز) به بخش‌های مختلف (سهم) تقسیم شده و هر سهم در اختیار یکی از واحدهای محاسبه‌گر قرار می‌گیرد به طوری که هیچکدام از آن‌ها نمی‌توانند به تنهایی از روی بخشی از داده که دریافت کرده‌اند به کل اطلاعات یا مقدار واقعی آن دسترسی پیدا کنند. اشتراک‌گذاری راز شمیر[6] یکی از این روش‌ها است که بر اساس درون‌یابی لاگرانژ[7] عمل بازیابی راز از سهم‌های رمزشده را انجام می‌دهد [45]. به طور دقیق‌تر، فرض کنید که $n \geq 2$ واحد محاسبه‌گر یا سرور وجود دارند که با یکدیگر تبانی نخواهند کرد. روش به اشتراک‌گذاری راز شمیر با ایجاد یک چندجمله‌ای درجه t با ضرایب تصادفی، راز s را به n سهم تقسیم کرده و میان n سرور به اشتراک می‌گذارد به طوری‌که حداقل $t \in \{2, \dots, n\}$ سهم نیاز است تا بتوان با درون‌یابی لاگرانژ راز اولیه را بازیابی کرد. در آن t عدد آستانه نام دارد و به روش اشتراک‌گذاری راز روش آستانه‌ای (t, n) می‌گویند. این روش به اشتراک‌گذاری راز نسبت به عمل جمع هم‌ریخت است و می‌توان با ایجاد پروتکل‌های امن سایر اعمال ریاضی را نیز با همکاری سرورها با یکدیگر ایجاد کرد [46, 47]. ساده‌ترین حالت خاص در این روش زمانی است که $t = n = 2$ باشد، یعنی داده میان دو سرور تقسیم می‌شود و هر دو سهم برای بازسازی داده اصلی مورد نیاز است.

از ترکیب این روش‌ها به همراه برخی دیگر از تکنیک‌های رمزنگاری نظیر انتقال ناآگاهانه[8] می‌توان امکان محاسبات چندجانبه امن[9] را در سیستم سایبرفیزیکی ایجاد کرد. در این صورت گروهی از عامل‌ها می‌توانند با همکاری یکدیگر یک مجموعه محاسبات مشخص یا محاسبه‌ی یک تابع دلخواه را بدون آن‌که ورودی‌ها و خروجی‌های خصوصی خود را برای دیگر عامل‌ها افشا کنند انجام دهند [48].

بیشتر روش‌های رمزنگاری تنها بر روی مجموعه‌ی اعداد صحیح نامنفی با اندازه‌ی محدود به درستی پیاده‌سازی می‌شوند. از این‌رو، برای به کارگیری این روش‌ها در کاربردهای کنترلی نیاز است تا داده‌های موجود که عموماً به صورت اعداد حقیقی هستند به فضای اعداد صحیح مورد نظر تصویر شوند. قدم اول برای ایجاد این تصویر، تقریب اعداد حقیقی ممیز شناور[10] به مجموعه اعداد ممیز ثابت[11] $Q_{b,\gamma,\delta}$، با اندازه γ، پایه b و دقت δ مشخص است. سپس با ضرب b^{δ} در تمام اعداد مجموعه‌ی $Q_{b,\gamma,\delta}$، زیرمجموعه‌ای از مجموعه‌ی اعداد صحیح به دست می‌آید. در نهایت، با اعمال تابع $h(y) = y \bmod P,\ h: Z \to Z_P$ داده‌ی مورد نظر به فضای پیام اعداد صحیح نامنفی با اندازه محدود Z_P منتقل می‌شود، که در آن $Z_P \triangleq \{0,1, \dots, P-1\}$ و P یک عدد به اندازه‌ی کافی بزرگ دلخواه است. انتخاب P باید به گونه‌ای باشد که فضای پیام را به خوبی پوشش دهد. توجه کنید که اندازه P در روش‌های هم‌ریختی مانند روش پیلیر در میزان امنیت روش تاثیرگذار است، اما در روش‌های به اشتراک‌گذاری راز اهمیتی ندارد. به همین دلیل، روش‌های هم‌ریختی طول داده‌ی بزرگتر و بار محاسباتی بالاتری دارند [18, 49]. توجه کنید که معکوس عمل کوآنتیده[12] کردن فوق در حالت کلی ممکن نیست. بنابراین نمی‌توان دوباره داده‌ی اولیه x را بازیابی کرد و تنها تقریبی از آن یعنی $\hat{x}$ به دست می‌آید. از این رو خطای کوآنتیده کردن همواره جزئی از فرآیند رمزنگاری در حوزه‌ی اعداد صحیح است. برای کاهش این خطا می‌توان دقت کوآنتیده کردن را افزایش داد که البته این موضوع باعث بزرگتر شدن عدد صحیح حاصل و بیشتر شدن بار محاسباتی می‌شود [18, 49, 50].

اخیراً پژوهش‌های متنوعی در موضوع کنترل رمزنگاری شده انجام شده است. این پژوهش‌ها در نوع روش رمزنگاری و کنترل‌کننده‌ی مورد بررسی با یکدیگر متفاوت هستند. علاوه بر آن، ساختارهای متفاوتی نیز برای سیستم سایبرفیزیکی در نظر گرفته شده که در آن یک فضای ابری، یا یک شبکه از چندین فضای ابری در یک ساختار توزیع شده برای انجام محاسبات وجود دارند. در ادامه، برخی از این کارهای انجام شده مرور می‌شوند.

۳-۳. کنترل‌کننده‌های خطی رمزنگاری شده

یکی از نخستین موارد کنترل رمزنگاری شده در [51] ارائه شده است که در آن یک کنترل‌کننده‌ی خطی توسط روش رمزنگاری هم‌ریختی ضربی الجمال پیاده‌سازی شده است. از مشکلات روش الجمال، بار محاسباتی بالا و تعداد زیاد رمزگشایی‌های مورد نیاز در سطح عملگر است. پایداری این روش با انجام تغییراتی، در [52] اثبات شده است. استفاده از روش پیلیر مشکل تعداد زیاد رمزگشایی‌های مورد نیاز در روش الجمال را ندارد. از این‌رو در بسیاری از موارد از این روش بهره گرفته شده است. در

[1] Somewhat homomorphic
[2] Leveled homomorphic
[3] Bootstrapping
[4] Message space
[5] Secret sharing
[6] Shamir
[7] Lagrange interpolation
[8] Oblivious transfer
[9] Secure multi-party computation
[10] Floating point
[11] Fixed point
[12] Quantize

[53] یک کنترل فیدبک خروجی با این روش رمزنگاری طراحی شده است و در [50] به یک ساختار کنترل شبکه‌ای تعمیم داده شده است. همچنین، پیاده‌سازی عملی دیجیتال این کنترل‌کننده‌ی خطی رمزنگاری شده در [38] ارائه شده است.

مرجع [49] با استفاده از روش اشتراک‌گذاری راز در یک ساختار محاسبات چندجانبه امن و با در نظر گرفتن دو فضای ابری مجزا توانسته است یک کنترل‌کننده‌ی فیدبک حالت رمزنگاری شده را پیاده‌سازی کند. این روش در [54] با بهره‌گیری از رمزنگاری پیلیر به کنترل‌کننده‌ی غیرخطی چندجمله‌ای نیز تعمیم داده شده است. استفاده از رمزنگاری هم‌ریختی پیلیر در ساختارهای محاسبه‌ی چندجانبه بار محاسباتی زیادی را به همراه دارد. به همین دلیل، مرجع [55] کنترل‌کننده‌ی چندجمله‌ای رمزنگاری شده را تنها با استفاده از یک ساختار چندجانبه مبتنی بر اشتراک‌گذاری راز ارائه کرده است.

اجرای کنترل رمزنگاری شده با رمزنگاری‌های هم‌ریختی برای کنترل‌کننده‌های دارای دینامیک که در آن‌ها برای به دست آوردن مقادیر بردار حالت کنترل‌کننده نیاز به تکرار محاسبات رمزنگاری شده در سطح کنترل‌کننده است با چالش بزرگ شدن فضای پیام رمزشده و در نهایت سرریز داده رو به رو است [21, 56]. این مشکل را می‌توان با بازنشانی دوره‌ای حالت‌های داخلی کنترل‌کننده به صفر یا ارسال حالت‌ها برای سیستم به منظور رمزگشایی و رمزنگاری مجدد در فضای پیام اولیه مرتفع کرد [21, 56]. اما این راه‌کارها ممکن است سطح عملکرد سیستم را کاهش داده یا در حالت دوم بار مخابراتی و محاسباتی زیادی را به سیستم تحمیل کنند. البته این مشکل تنها زمانی رخ می‌دهد که ضرایب معادله مشخصه کنترل‌کننده اعدادی غیرصحیح باشند. بنابراین، مرجع [57] راه‌کار مشکل عمر محدود کنترل‌کننده‌های رمزنگاری شدی دارای دینامیک را ارائه‌ی کنترل‌کننده‌هایی با ضرایب عدد صحیح دانسته و روشی برای یافتن کنترل‌کننده‌ی معادل با ضرایب صحیح برای یک کنترل‌کننده مرتبه اول با ضرایب غیرصحیح ارائه کرده است. اما نویسندگان [58] نشان دادند که کنترل‌کننده‌های خطی با ضرایب عدد صحیح عموماً ناپایدار هستند و تنها تعداد محدودی با پایداری مرزی از این کنترل‌کننده‌ها را برشمرده‌اند. در ادامه، در [59] تلاش شد که با کمک گرفتن از تحقق‌های غیرکمینه، دایره‌ی کنترل‌کننده‌های پایدار اما دارای ضرایب صحیح را گسترده‌تر کنند. بررسی دقیق‌تر این موضوع هنوز ادامه دارد [60, 61].

۳-٤. کنترل پیش‌بین رمزنگاری شده

تاکنون تلاش‌هایی برای طراحی کنترل‌کننده‌های پیش‌بین رمزنگاری شده انجام شده است. یکی از چالش‌های اصلی اعمال روش‌های رمزنگاری بر روش‌های کنترلی پیچیده‌تر این است که خاصیت هم‌ریختی در بسیاری از روش‌های رمزنگاری تنها بر روی عملیات‌های محدودی برقرار است. پیچیدگی زیاد محاسبات برای حل بهینه‌سازی موجود در ساختار کنترل پیش‌بین باعث شده است که در تلاش‌های اولیه تنها از کنترل پیش‌بین صریح[1] با محاسبات برون‌خط[2] استفاده شود [62, 63]. در واقع در این روش‌ها، کنترل‌کننده‌ی پیش‌بین به چندین کنترل‌کننده‌ی فیدبک حالت با بهره‌های از پیش محاسبه شده تبدیل می‌شود و سپس نتایج موجود برای کنترل‌کننده‌های خطی رمزنگاری شده برای پیاده‌سازی قانون کنترل پیش‌بین رمزنگاری شده تعمیم داده می‌شود.

به منظور حل برخط[3] مسئله‌ی بهینه‌سازی کنترل پیش‌بین به صورت رمزنگاری شده، یک راه‌کار مشترک در مراجع، تبدیل مسئله‌ی کنترل پیش‌بین به یک مسئله‌ی بهینه‌سازی مربعی و سپس اتخاذ یک الگوریتم حل مرتبه اول است که پیچیدگی محاسباتی زیادی نداشته باشد [70-64]. در [64] مسئله‌ی بهینه‌سازی به روش گرادیان تصویر شده‌ی سریع[4] حل شده است. در این مرجع، تنها حالت‌های سیستم و کران محدودیت ورودی به صورت رمز شده هستند. ماتریس‌های مدل سیستم و پارامترهای کنترل‌کننده بدون رمزنگاری در مسئله استفاده شده‌اند. به این ترتیب، تکرارهای حل مسئله‌ی بهینه‌سازی با اعمال خاصیت هم‌ریختی عمل جمع در رمزنگاری پیلیر قابل پیاده‌سازی است. هر چند عمل غیرخطی تصویر کردن گرادیان حاصل شده، که در حالت ساده‌ی بازه‌ای بودن محدودیت‌ها به مسئله‌ی مقایسه دو عدد تبدیل می‌شود، قابل انجام بر روی داده‌های رمز شده نیست. بنابراین در هر تکرار، مقدار گرادیان محاسبه شده که به صورت رمز شده است به سطح سیستم فرستاده می‌شود و در آن‌جا بعد از رمزگشایی، عمل تصویر کردن با داده‌های بدون رمز انجام شده و سپس دوباره برای ارسال به واحد محاسبه‌گر ابری رمزنگاری می‌شود. این کار بار محاسباتی زیادی را بر سیستم تحمیل می‌کند زیرا در هر گام نمونه‌برداری سیستم علاوه بر انجام عمل تصویر کردن باید بارها عمل رمزگشایی و رمزنگاری را انجام دهد. یک راه‌کار که در [65] پیشنهاد شده است، انجام تنها یک تکرار از مسئله‌ی بهینه‌سازی است. در این روش، عمل تصویر کردن در سطح عملگر سیستم انجام می‌شود. اما از آن‌جایی که تنها یک تکرار از حل مسئله‌ی بهینه‌سازی انجام می‌شود، نیازی به دوباره رمزنگاری کردن متغیر تصویر شده و ارسال آن به کنترل‌کننده ابری وجود ندارد. به این ترتیب، پیچیدگی روش و بار محاسباتی سیستم تا حد زیادی کاهش می‌یابد، اما عملکرد حلقه‌بسته تحت‌الشعاع قرار می‌گیرد. ایده تنها یک‌بار حل مسئله‌ی بهینه‌سازی در [66] برای بهینه‌سازی به روش جهت متناوب ضرایب[5] (ADMM) به کار گرفته شده است. به این ترتیب، علاوه بر قید ورودی، قید حالت نیز در مسئله لحاظ شده است.

راه‌کار دیگری که برای حل مشکل فوق پیشنهاد شده است، اضافه کردن یک واحد محاسباتی کمکی در فضای ابری است [67]. در این روش، یک واحد هدف[6] با امکانات محاسباتی بیشتر از سیستم در ساختار مسئله در نظر گرفته شده است. در این ساختار، فرض می‌شود که واحد محاسبه‌گر اصلی و واحد کمکی با یکدیگر تبانی[7] نخواهند کرد، اما هر کدام مایل هستند که به داده‌های واقعی سیستم دسترسی پیدا کنند. از آن‌جایی که واحد محاسبه‌گر کمکی نیز نباید از مقدار اصلی متغیر

[1] Explicit model predictive control
[2] Offline
[3] Online
[4] Projected fast gradient method
[5] Alternating Direction Method of Multipliers (ADMM)
[6] Target node
[7] Collude

بهینه‌سازی مطلع شود، روش‌های مختلفی برای مخفی کردن مقدار اصلی اعداد رمزنگاری شده در مراجع مختلف استفاده شده است [67, 68]. نتایج پیاده‌سازی عملی این روش در [69] گزارش شده است. تمام موارد مطرح شده، از رمزنگاری پیلیر در محاسبه سیگنال کنترلی استفاده کرده‌اند. میزان خصوصی ماندن اطلاعات در روش پیلیر یا سایر روش‌های هم‌ریختی مشابه در دشوار بودن محاسباتی روند ریاضی سازنده‌ی رمز است. بنابراین، میزان امنیتی که ایجاد می‌کنند به طول کلید خصوصی رمزنگاری بستگی دارد. از طرفی بالا بردن طول کلید، باعث افزایش بار محاسباتی روش و افزایش حافظه‌ی مورد نیاز می‌شود. در مقابل، روش‌های به اشتراک‌گذاری راز می‌توانند بدون این محدودیت، در یک فضای پیام کوچک‌تر و بار محاسباتی کم‌تر امنیت کامل را ارائه کنند [49].

با توجه به موارد فوق، در [70] از روش اشتراک‌گذاری راز برای برون‌سپاری محاسبات لازم برای حل مسئله‌ی بهینه‌سازی کنترل پیش‌بین استفاده شده است. همچنین، به منظور حذف خطاهای ناشی از کوآنتیده کردن سیگنال‌ها در یک سیستم کنترلی و جلوگیری از مشکلات ناشی از کار بر روی اعداد صحیح مثبت در فضای محدود مانند سرریزکردن یا اجرای عمل تقسیم، در این پژوهش از یک روش اشتراک‌گذاری راز مبتنی بر اعداد حقیقی استفاده شده است. از طرف دیگر، انجام عمل مقایسه‌ی دو مقدار رمز شده که در عمل تصویر کردن روش گرادیان تصویر شده[1] مورد نیاز است، به طور کامل در سطح فضای ابری و با کمک سرورهای محاسباتی با حفظ حریم خصوصی انجام می‌شود و نیازی به واحد هدف یا بازگرداندن محاسبات به سطح سیستم وجود ندارد. مدل سیستم، حالت اولیه و مسیر حالت سیستم، سیگنال کنترلی ورودی و تمام قیدهای سیستم به عنوان داده حساس در نظر گرفته شده که باید در تمام مراحل محاسبه‌ی کنترل‌کننده و تمام حلقه‌ی کنترل خصوصی باقی بماند. همچنین، نیاز است تا مقدار متغیرهای میانی در گام‌های داخلی حل مسئله‌ی بهینه‌سازی که ممکن است به افشا شدن مقدار بهینه‌ی سیگنال کنترلی منجر شود نیز به صورت رمز شده باشند. تمام داده‌های حساس به چندین سهم رمزنگاری شده تقسیم شده و در اختیار هرکدام از سرورها قرار می‌گیرند. سپس تمام محاسبات لازم توسط سرورها، به طور مستقیم بر روی این سهم‌ها انجام شده و سرورها تحت پروتکل‌های روش اشتراک‌گذاری راز با یکدیگر همکاری می‌کنند تا مسئله‌ی بهینه‌سازی را حل کنند. پاسخ نهایی که به صورت رمزنگاری شده و شامل سهم‌های هر کدام از سرورها از سیگنال کنترلی است برای عملگر سیستم فرستاده می‌شود. این سهم‌ها در سطح عملگر به سیگنال اصلی بازیابی شده و به سیستم اعمال می‌گردند. بنابراین، سیگنال‌های حساس به محض خروج از سنسور تا بازگشت دوباره به سطح عملگر در سیستم به صورت رمزنگاری شده باقی می‌مانند.

۳-۵. کنترل و بهینه‌سازی توزیع‌یافته رمزنگاری شده

به منظور حل امن مسئله‌های توزیع‌یافته و غیرمتمرکز لازم است که گروهی از عامل‌ها با به اشتراک گذاشتن اطلاعات رمزنگاری شده، تابع مشترکی را محاسبه کنند یا محاسبات لازم برای یک مسئله‌ی بهینه‌سازی به بخش‌های مختلف تجزیه شده و هر بخش را یک عامل محاسبه‌کننده‌ی مجزا انجام دهد، بدون آن‌که از مقدار واقعی محاسبه‌شده توسط سایر اجزا مطلع شود.

مرجع [71] حریم خصوصی عامل‌ها در یک مسئله بهینه‌سازی غیرمتمرکز را با استفاده از اشتراک‌گذاری راز و طراحی یک ساختار چندجانبه امن برای حل مسئله‌ی بهینه‌سازی به روش ADMM حفظ کرده است. البته در ساختار ارائه شده به یک ناظر معتمد برای بررسی قیدها نیاز است که فرض غیرمطلوبی محسوب می‌شود. مرجع [72] مسئله‌ی بهینه‌سازی توزیع‌یافته را به بخش عمومی و بخش محلی تقسیم کرده و بخش عمومی بدون نیاز به داشتن هیچ مرکز معتمد و تنها با استفاده از روش اشتراک‌گذاری راز حل می‌شود. مرجع [73] با استفاده از ترکیبی از روش‌های رمزنگاری هم‌ریختی و اشتراک‌گذاری راز، روشی توزیع‌یافته با حفظ حریم خصوصی برای محاسبه‌ی چندجمله‌ای‌ها در شبکه‌ای از عامل‌ها ارائه کرده است. در [74] عامل‌های موجود در یک گراف به هم پیوسته می‌توانند تنها با انتقال اطلاعات رمزنگاری شده میان عامل‌های همسایه، حاصل‌جمع اطلاعات تمام شبکه را محاسبه کنند بدون اینکه هیچ کدام از عامل‌ها به اطلاعات محرمانه‌ی عامل دیگر دست یابد. مسئله‌ی کنترل تجمعی که با فیدبک‌های ساختاریافته مدل شده، در [75] بررسی شده است. مسئله‌ی بهینه‌سازی توزیع‌یافته به روش گرادیان تصویر شده با استفاده از رمزنگاری هم‌ریختی پاره‌ای در [76] ارائه شده و برای کنترل رمزنگاری شده توان بهینه در شبکه‌ی قدرت استفاده شده است [76, 77].

در [78] از روش اشتراک‌گذاری راز که بار محاسباتی کمتر اما پیچیدگی مخابراتی بیشتری دارد برای حفظ حریم خصوصی در مسئله‌ی بهینه‌سازی توزیع‌یافته‌ی شارژ خودروهای الکتریکی استفاده شده است. در این مسئله، عامل‌ها برای حل بهینه‌سازی محلی مربوط به خود تنها نیاز به مجموع شارژ عامل‌های دیگر دارند. این مجموع به راحتی با استفاده از خاصیت هم‌ریختی جمعی در روش اشتراک‌گذاری راز انجام می‌شود. اما محاسبه‌ی مشترک توابع پیچیده‌تر به صورت مشارکتی توسط عامل‌ها نیاز به بررسی بیشتری دارد. مسئله‌ی اجماع میانگین دسته‌ای از عامل‌های با دینامیک مرتبه دو با حفظ حریم خصوصی هر کدام از عامل‌ها توسط رمزنگاری پیلیر در [79] بررسی شده است.

۳-۶. تخمین حالت رمزنگاری شده

علاوه بر طراحی کنترل‌کننده، تخمین حالت‌ها به صورت رمزنگاری شده نیز مورد توجه است. در [80] مسئله‌ی تخمین حالت‌های سیستم با ایجاد یک مدل رمزنگاری ترکیبی از روش الجمال و روش پیلیر بررسی شده است. در [81] از روش رمزنگاری پیلیر برای طراحی یک رویت‌گر رمزنگاری شده و کنترل‌کننده‌ی مبتنی بر آن استفاده شده است تا از حمله‌های استراق سمع جلوگیری شود و در [82] الگوریتمی برای تشخیص خطای تزریق داده‌ی اشتباه نیز به نتایج قبل اضافه شده است. در [83] از

[1] Projected gradient method

رمزنگاری پیلیر برای طراحی فیلتر کالمن امن استفاده شده است. حفظ حریم خصوصی در مسئله‌ی تخمین حالت مبتنی بر مجموعه‌ها[1] که در محاسبه‌ی مجموعه حالت‌های ایمن در سیستم‌های بحرانی نسبت به ایمنی[2] کاربرد دارد در [84] بررسی شده است. پارامترهای مشخص کننده‌ی مجموعه با رمزنگاری پیلیر رمز شده و رویت‌گر مبتنی بر مجموعه رمزنگاری شده که در آن هم داده‌های سیستم و هم کران مجموعه‌ی تخمین زده شده خصوصی باقی می‌مانند طراحی شده است. مشکل سرریز شدن داده‌ی رمز شده از فضای پیام رمزنگاری شده که در بسیاری از کابردهای رمزنگاری هم‌ریختی وجود دارد در [84] دیده می‌شود. در این مقاله، در هر مرحله مجموعه‌ی تخمین زده شده به یک عامل قابل اعتماد فرستاده شده و در آن رمزگشایی شده و دوباره رمزنگاری می‌شود تا مشکل بزرگ شدن فضای پیام به وجود نیاید.

۳-۷. کاربرد کنترل رمزنگاری شده

استفاده از کنترل رمزنگاری شده در کاربردهای عملی نیر مورد توجه پژوهشگران قرار گرفته است. کنترل پیش‌بین رمزنگاری شده برای حل مسئله‌ی دنبال کردن مسیر برای یک پرنده‌ی بدون سرنشین کنترل‌پذیر از راه دور که توسط یک کنترل‌کننده‌ی برخط هدایت می‌شود در [85] بررسی شده است. هر چند در این مقاله، به منظور کاهش بار محاسباتی، تنها کنترل حرکت عمودی پرنده به طور کامل توسط کنترل رمزنگاری شده انجام می‌شود و حرکت در صفحه به کمک یک کنترل‌کننده رمزنشده محلی صورت می‌گیرد. مسئله‌ی هدایت رمزنگاری شده قایق‌های خودران توسط هدایتگر مستقر در فضای ابری در [86] بررسی شده است. در واقع با اعمال یک رمزنگاری هم‌ریختی جمعی قانون هدایت به طوری محاسبه می‌شود که موقعیت و مسیر قایق برای واحد هدایتگر افشا نمی‌شود.

مسئله‌ی حفظ حریم خصوصی در سیستم‌های سلامت و کنترل دستگاه‌های الکترونیکی قابل کاشت در بدن مورد توجه قرار گرفته و استفاده از رمزنگاری برای رسیدن به این منظور پیشنهاد شده است [87, 88]. مرجع [89] خصوصی نگه‌داشتن اطلاعات بیمار در هنگام کنترل قند خون توسط یک کنترل‌کننده PID در یک پانکراس مصنوعی را با یک روش رمزنگاری هم‌ریختی مطالعه کرده است.

به عنوان نمونه‌ای از استفاده از روش‌های رمزنگاری در کنترل ترافیک می‌توان به [90] اشاره کرد که در آن از روش اشتراک‌گذاری راز برای محاسبه‌ی امن زمان سبز چراغ‌های راهنمایی با روش‌های یادگیری عمیق استفاده شده است. در [91] رمزنگاری هم‌ریختی به عنوان یک راه‌کار حفظ حریم خصوصی در اجرای برون‌سپاری شده‌ی عملیات نگه‌داری و تعمیرات پیش‌گیرانه یک واحد صنعتی به کار گرفته شده است.

٤- چالش‌های کنترل رمزنگاری شده و مسیر پژوهش‌های آینده

هرچند روش‌های رمزنگاری هم‌ریختی از مدت‌ها پیش مطرح شده و در کاربردهای مربوط به سیستم‌های فناوری اطلاعات و پردازش داده به کار گرفته شده‌اند، استفاده از آن‌ها در ساختار سیستم‌های کنترل و ایجاد روش‌های کنترل رمزنگاری شده بسیار نوپا است. مرور پژوهش‌های اخیر نشان می‌دهد که کماکان چالش‌های متعددی در ایجاد الگوریتم‌های کارآمد در حوزه‌ی کنترل رمزنگاری شده و گسترش کاربرد آن به ساختارهای کنترلی پیچیده‌تر وجود دارد. به برخی از این چالش‌ها در ادامه اشاره شده و چشم‌انداز پژوهش‌های بیشتر برای حل این موانع ترسیم شده است.

٤-١. کوآنتیده کردن سیگنال‌ها و خطای ناشی از آن

برای طراحی کنترل رمزنگاری شده نیاز است تا سیگنال‌ها و پارامترهای کنترل‌کننده کوآنتیده شوند. همچنین حساب پیمانه‌ای[3] لازم برای اجرای روش‌های رمزنگاری ایجاب می‌کند تا سیگنال‌ها به فضای اعداد صحیح نامنفی با بعد محدود تصویر شوند. کوآنتیده کردن سیگنال‌ها ممکن است موجب کاهش عملکرد سیستم یا حتی از دست رفتن پایداری سیستم شود [92, 93]. کران بالایی برای میزان کاهش عملکرد سیستم رمزنگاری شده نسبت به سیستم بدون رمزنگاری با فرض رمزنگاری الجمال و کنترل‌کننده‌ی خطی برای یک سیستم خطی در [94] ارائه شده است. در [95] با گسترش فضای اطلاعات آشکار روش رمزنگاری الجمال به دربر گرفتن صفر و اعداد منفی، یک روش کوآنتیده کردن پویا ارائه شده است تا خطای خروجی سیستم کنترل رمزنگاری شده و رمز نشده را حداقل نماید. به این ترتیب عملکرد حلقه‌بسته بهبود یافته است.

برخی مراجع تلاش کرده‌اند تا رمزنگاری به روش اشتراک‌گذاری راز را به طور مستقیم بر روی اعداد حقیقی انجام دهند [47, 96]. در این روش از توابع متعامد لاگرانژ به جای حساب پیمانه‌ای در یک ساختار اشتراک‌گذاری راز استفاده شده است که در آن نیازی به تبدیل سیگنال‌ها به اعداد صحیح وجود ندارد و به این ترتیب خطاهای ناشی از کوآنتیده کردن و بار محاسباتی مربوط به آن از بین می‌رود. برخلاف روش‌های مبتنی بر اعداد صحیح در میدان محدود که در آن اعداد تصادفی دارای توزیع یکنواخت هستند، اعداد تصادفی مورد نیاز در این روش را می‌توان از میان اعداد حقیقی با توزیع گوسی انتخاب کرد. هرچند این موضوع مانع از دست‌یابی به امنیت کامل در این روش می‌شود، اما نشان داده شده است که میزان درز اطلاعات در این روش را می‌توان با انتخاب درست پارامترها کنترل کرد.

با توجه به مطالب فوق، بررسی دقیق اثر خطاهای ناشی از کوآنتیده کردن در ساختار کنترل، با استفاده از مفاهیم کنترل مقاوم یکی از مسائل مهم پیش رو در بحث کنترل رمزنگاری شده است. این مسیر پژوهشی کمک خواهد کرد تا روش‌هایی با تضمین پایداری و همگرایی در حضور خطاهای ناشی از رمزنگاری به دست آید.

٤-٢. محدودیت‌های ناشی از رمزنگاری‌های هم‌ریختی

در بخش قبل دیدیم که استفاده از روش‌های رمزنگاری هم‌ریختی محدودیت‌های بسیاری دارد. عموم روش‌های کنترل رمزنگاری شده که تاکنون ارائه شده‌اند محدود به کنترل‌کننده‌های ساده با فرض‌های بسیار

[1] Set-based estimation
[2] Safety critical systems
[3] Modular arithmetic

ایده‌آل گرایانه هستند. در واقع حتی با کمک روش‌های هم‌ریختی کامل، ایجاد ساختارهای غیرخطی یا ساختارهای شرطی که در بسیاری از روش‌های کنترلی وجود دارد، دشوار خواهد بود. از این رو نیاز است تا در هنگام ارائه روش‌های جدید سعی شود تا تغییرات لازم در روش‌های کنترلی را طوری اعمال کرد که محدودیت‌های ساختاری کمتری ایجاد شود. به عبارت دیگر، ضروری است تا با طراحی توامان روش کنترلی و روش رمزنگاری، ترکیبی را انتخاب کرد که قابلیت‌های بیشتری ارائه می‌دهد.

بار محاسباتی زیاد یکی از مشکلات مهم در به کارگیری روش‌های کنترل رمزنگاری شده است. روش‌های مرتبط با کاهش بار محاسباتی خود روش‌های رمزنگاری در بخش‌های قبل اشاره شد. راه‌کار دیگر، استفاده از مفاهیم کاهش بار محاسباتی مرسوم در مهندسی کنترل خواهد بود. به عنوان مثال، در [97] با استفاده از یک راه‌کار رویداد پایه[1] برای کاهش نرخ بیت در انتقال داده میان بخش‌های سیستم و در نتیجه افزایش دوره‌ی نمونه‌برداری سیستم در برخی از زمان‌ها، از ایجاد تاخیر ناشی از رمزنگاری جلوگیری شده است.

موضوع دیگر، بزرگ‌شدن مقادیر رمزشده در هنگام محاسبه‌ی کنترل‌کننده‌های دارای دینامیک به صورت رمزنگاری شده است که یافتن راه‌کار مناسبی که جامعیت بیشتری داشته باشد نیازمند پژوهش بیشتری است.

در بحث محاسبه‌ی چندجانبه‌ی امن و روش‌های مبتنی بر اشتراک‌گذاری راز، یکی از موارد مهم که تاکنون در تمام مراجع نادیده گرفته شده، اثر تاخیر هر کدام از سرورها در انجام محاسبات و همگام نبودن آن‌ها با یکدیگر در عملکرد و پایداری سیستم‌های کنترل رمزنگاری شده است. بنابراین، ضروری به نظر می‌رسد تا استفاده از روش‌های محاسبه‌ی چندجانبه‌ی امن با سرورهای غیرهمگام [98] در ساختارهای کنترلی مطالعه شود.

٤-٣. حمله‌های فعال بر سیستم‌های کنترل رمزنگاری شده

هرچند رمزنگاری می‌تواند خصوصی ماندن اطلاعات را در حلقه‌ی کنترل تضمین کند، اما کماکان عامل‌های خرابکار می‌توانند بدون رمزگشایی یا دانستن مقدار واقعی سیگنال رمز شده، آن را دستکاری کنند و به این ترتیب کیفیت پاسخ کنترل رمزنگاری شده دچار تغییر می‌شود [102-99]. یک روش رمزنگاری که نسبت به عمل ضرب ماتریس در یک بردار هم‌ریخت است در [99] ارائه شده است که از آن می‌توان برای دسته‌ای از روش‌های کنترل رمزنگاری شده که در آن کنترل‌کننده به صورت ضرب یک بردار در ماتریس تبدیل می‌شود استفاده کرد. این روش علاوه بر حفظ خصوصی بودن داده‌های سیستم و پارامترهای کنترل‌کننده، نسبت به حمله‌ی تزریق داده اشتباه به صورت جمع‌شونده در خروجی سیستم تاب‌آور است. یعنی این حمله در خروجی رمزگشایی شده‌ی کنترل‌کننده تاثیری نخواهد داشت. حد تاب‌آوری کنترل رمزنگاری شده در [99] محدود بوده و حمله‌های شدیدتر پاسخ سیستم را دچار تغییر خواهند کرد. از این رو، در [100] راه‌کاری برای تشخیص حمله بر روی سیستم رمزنگاری شده و قدرت آن پیشنهاد شده است. رهیافت دیگری بر اساس رمزنگاری هم‌ریختی ضربی در [101] پیشنهاد شده است تا بتواند حمله‌های تزریق داده‌ی اشتباه به سیگنال‌های رمز شده در ساختار کنترل‌کننده را به صورت برخط تشخیص داده و مکانیزم دفاعی برای کاهش اثر آن را فعال کند. همچنین، در [102] نشان داده شده است که یک عامل خرابکار می‌تواند تحت شرایطی مانند امکان ایجاد تغییر در ماژول تولید اعداد تصادفی در ساختار کنترل رمزنگاری‌شده با رمزنگاری الجمال و پیلیر، خصوصی بودن داده‌های رمز شده را از بین ببرد. بنابراین، بررسی آسیب‌پذیری‌های سیستم‌های کنترل رمزنگاری شده در مقابل حملات فعال یکی از دغدغه‌های مهم در توسعه کاربرد این روش‌ها است که تاکنون جز در موارد محدود با فرضیات ساده برای حالت‌های پیچیده‌تر بررسی نشده و نیاز به مطالعه و بررسی بیشتری دارد.

٤-٤. اعمال روش‌های کنترل رمزنگاری شده به کاربردهای عملی

عموم تلاش‌های انجام شده برای گسترش دایره‌ی کاربرد روش‌های کنترل رمزنگاری شده برای حفظ حریم خصوصی در کاربردهای عملی که تاکنون ارائه شده، بیشتر با هدف نشان دادن اثربخشی این روش‌ها و اهمیت آن‌ها در کاربرد مورد نظر بوده و از لحاظ عملی قابل قبول نیست. با پیشرفت دانش نظری در طراحی کنترل‌کننده‌های رمزنگاری شده، به طور همزمان می‌توان به جزییات اعمال این روش‌ها در کاربردهای عملی پرداخت به طوری که در عمل قابل پیاده‌سازی باشد.

٥- نتیجه‌گیری

این مقاله یک مطالعه‌ی مروری بر موضوع امنیت سیستم‌های سایبرفیزیکی و به طور مشخص روش‌های حفظ حریم خصوصی با کنترل رمزنگاری شده را ارائه کرد. ابتدا اهمیت بررسی امنیت سایبری در سیستم‌های شبکه‌ای و سایبرفیزیکی بیان شد و یک دسته‌بندی از انواع حمله‌ها با توجه به هدف و ماهیت خرابکارانه‌ی آن‌ها ارائه شد. در ادامه، مفهوم کنترل رمزنگاری شده که به منظور پیش‌گیری از وقوع حملات سایبری توسعه یافته است، تشریح شد. چند نمونه از روش‌های رمزنگاری و تلاش‌هایی که تاکنون برای استفاده از این روش‌ها در ساختارهای کنترلی انجام شده است مرور شد. در این روش‌ها علاوه بر انتقال سیگنال‌ها میان اجزا (از سنسور به کنترل‌کننده و از کنترل‌کننده به عملگر) که به صورت رمزشده انجام می‌شود، تمام محاسبات لازم برای محاسبه‌ی سیگنال کنترلی نیز بر روی سیگنال رمزنگاری شده انجام می‌شود و نیازی به باز کردن رمز و در معرض خطر قرار دادن اطلاعات مهم وجود ندارد. این کار امکان دسترسی حمله‌کننده‌ها به اطلاعات حیاتی سیستم کنترلی را بسیار محدود می‌کند. همچنین از آن‌جایی که برای طراحی حملات پیچیده‌تر، عموماً به اطلاعات به دست آمده از سیستم نیاز است، حفظ خصوصی بودن سیگنال‌ها در تمام حلقه‌ی کنترل، احتمال طرح حمله‌های سایبری پیچیده‌تر را نیز به طور قابل ملاحظه‌ای کاهش می‌دهد. در نهایت، به برخی از چالش‌های موجود در گسترش دانش نظری و کاربردی کردن روش‌های

[1] Event-triggered

کنترل رمزنگاری شده اشاره شد و پیشنهادهایی برای ادامه‌ی پژوهش در این زمینه معرفی شد.

تشکر و قدردانی

این اثر تحت حمایت مادی صندوق حمایت از پژوهشگران و فناوران کشور (INSF) برگرفته شده از طرح شماره «۴۰۰۴۹۱۵» انجام شده است.

مراجع

[1] Xia, Y., Zhang, Y., Dai, L., Zhan, Y., & Guo, Z. (2022). A brief survey on recent advances in cloud control systems. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 69(7), 3108-3114.

[2] Zhang, D., Wang, Q.G., Feng, G., Shi, Y., & Vasilakos, A.V. (2021). A survey on attack detection, estimation and control of industrial cyber-physical systems. *ISA transactions*, 116, 1-16.

[3] Dibaji, S.M., Pirani, M., Flamholz, D.B., Annaswamy, A.M., Johansson, K.H., & Chakrabortty, A. (2019). A systems and control perspective of CPS security. *Annual Reviews in Control*, 47, 394-411.

[4] Sandberg, H., Gupta, V., & Johansson, K.H. (2022). Secure networked control systems. *Annual Review of Control, Robotics, and Autonomous Systems*, 5, 445-464.

[5] Teixeira, A., Sou, K.C., Sandberg, H., & Johansson, K.H. (2015). Secure control systems: A quantitative risk management approach. *IEEE Control Systems Magazine*, 35(1), 24-45.

[6] Nekouei, E., Tanaka, T., Skoglund, M., & Johansson, K. H. (2019). Information-theoretic approaches to privacy in estimation and control. *Annual Reviews in Control*, 47, 412-422.

[7] Lu, Y., & Zhu, M. (2019). A control-theoretic perspective on cyber-physical privacy: Where data privacy meets dynamic systems. *Annual Reviews in Control*, 47, 423-440.

[8] Sánchez, H. S., Rotondo, D., Escobet, T., Puig, V., & Quevedo, J. (2019). Bibliographical review on cyber-attacks from a control-oriented perspective. *Annual Reviews in Control*, 48, 103-128.

[9] Li, G., Ren, L., Fu, Y., Yang, Z., Adetola, V., Wen, J., Zhu, Q., Wu, T., Candan, K.S. & O'Neill, Z. (2023). A critical review of cyber-physical security for building automation systems. *Annual Reviews in Control*, 55, 237-254.

[10] Arauz, T., Chanfreut, P., & Maestre, J. M. (2022). Cyber-security in networked and distributed model predictive control. *Annual Reviews in Control*, 53, 338-355.

[11] Blanco-Justicia, A., Domingo-Ferrer, J., Martínez, S., Sánchez, D., Flanagan, A., & Tan, K. E. (2021). Achieving security and privacy in federated learning systems: Survey, research challenges and future directions. *Engineering Applications of Artificial Intelligence*, 106, 104468.

[12] Afshar, A., Termehchy, A., Golshan, A., Aghaeeyan, A., & Shahriyari, H. (2014). Survey on cyber security of industrial control systems. *Journal of Control*, 8(1), 31-45.

[13] Cheng, Z., Ye, F., Cao, X., & Chow, M.Y. (2021). A homomorphic encryption-based private collaborative distributed energy management system. *IEEE Transactions on Smart Grid*, 12(6), 5233-5243.

[14] Zhang, C. & Wang, Y. (2018). Enabling privacy-preservation in decentralized optimization. *IEEE Transactions on Control of Network Systems*, 6(2), 679-689.

[15] Huo, X. & Liu, M. (2021). Encrypted decentralized multi-agent optimization for privacy preservation in cyber-physical systems. *IEEE Transactions on Industrial Informatics*. In Press.

[16] Sharma, S. & Kaushik, B. (2019). A survey on internet of vehicles: Applications, security issues & solutions. *Vehicular Communications*, 20, 100182.

[17] Sultangazin, A. & Tabuada, P. (2020). Symmetries and isomorphisms for privacy in control over the cloud. *IEEE Transactions on Automatic Control*, 66(2), 538-549.

[18] Darup, M.S., Alexandru, A.B., Quevedo, D.E., & Pappas, G.J. (2021). Encrypted Control for Networked Systems: An Illustrative Introduction and Current Challenges. *IEEE Control Systems Magazine*, 41(3), 58-78.

[19] Suryavanshi, A., Alnajdi, A., Alhajeri, M., Abdullah, F., & Christofides, P. D. (2023). Encrypted model predictive control design for security to cyberattacks. *AIChE Journal*, 69(8), e18104.

[20] Sun, Q., & Shi, Y. (2021). Model predictive control as a secure service for cyber–physical systems: A cloud-edge framework. *IEEE Internet of Things Journal*, 9(22), 22194-22203.

[21] Kim, J., Kim, D., Song, Y., Shim, H., Sandberg, H., & Johansson, K.H. (2022). Comparison of encrypted control approaches and tutorial on dynamic systems using Learning With Errors-based homomorphic encryption. *Annual Reviews in Control*, 54, 200-218.

[22] Umsonst, D. & Sandberg, H. (2021). On the confidentiality of controller states under sensor attacks. *Automatica*, 123, 109329.

[23] An, L., & Yang, G.H. (2022). Enhancement of opacity for distributed state estimation in cyber–physical systems. *Automatica*, 136, 110087.

[24] Wang, L., Zhang, M., Zhu, J., Xing, L., & Wu, Q.

A., & Sanfelice, R. G. (2023). Online attack recovery in cyberphysical systems. *IEEE Security & Privacy*, 21(4), 20-28.

[38] Tran, J., Farokhi, F., Cantoni, M., & Shames, I. (2020). Implementing homomorphic encryption based secure feedback control. *Control Engineering Practice*, 97, 104350.

[39] ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4), 469-472.

[40] Paillier, P. (1999, May). Public-key cryptosystems based on composite degree residuosity classes. In *International conference on the theory and applications of cryptographic techniques*, (pp. 223-238). Springer, Berlin, Heidelberg.

[41] Gentry, C. (2009, May). Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, (pp. 169-178).

[42] Teranishi, K., Sadamoto, T., & Kogiso, K. (2023). Input-output history feedback controller for encrypted control with leveled fully homomorphic encryption. *IEEE Transactions on Control of Network Systems*, In press.

[43] Cheon, J.H., Kim, A., Kim, M., & Song, Y. (2017). Homomorphic encryption for arithmetic of approximate numbers. In *23rd International Conference on the Theory and Applications of Cryptology and Information Security*, Hong Kong, China, (pp. 409-437). Springer.

[44] Ducas, L., & Micciancio, D. (2015, April). FHEW: bootstrapping homomorphic encryption in less than a second. *In Annual international conference on the theory and applications of cryptographic techniques* (pp. 617-640). Berlin, Heidelberg: Springer.

[45] Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22(11), 612-613.

[46] Xia, Z., Gu, Q., Zhou, W., Xiong, L., Weng, J., & Xiong, N. (2021). STR: Secure computation on additive shares using the share-transform-reveal strategy. *IEEE Transactions on Computers*, In press.

[47] Tjell, K. & Wisniewski, R. (2021). Privacy in Distributed Computations based on Real Number Secret Sharing. *arXiv preprint arXiv:2107.00911*.

[48] Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C. Z., Li, H., & Tan, Y.A. (2019). Secure multi-party computation: theory, practice and applications. Information Sciences, 476, 357-372.

[49] Darup, M.S. & Jager, T. (2019, December). Encrypted cloud-based control using secret sharing with one-time pads. In *2019 IEEE 58th Conference on Decision and Control (CDC)*, (pp. 7215-7221).

(2022). A privacy-preserving decentralized randomized block-coordinate subgradient algorithm over time-varying networks. *Expert Systems with Applications*, 208, 118099.

[25] Murguia, C., Shames, I., Farokhi, F., Nešić, D., & Poor, H.V. (2021). On privacy of dynamical systems: An optimal probabilistic mapping approach. IEEE *Transactions on Information Forensics and Security*, 16, 2608-2620.

[26] Hassan, M.U., Rehmani, M.H., & Chen, J. (2019). Differential privacy techniques for cyber physical systems: a survey. IEEE Communications Surveys & Tutorials, 22(1), 746-789.

[27] Wang, Y., & Nedić, A. (2023). Tailoring gradient methods for differentially-private distributed optimization. *IEEE Transactions on Automatic Control*, In press.

[28] Chen, B., Leahy, K., Jones, A., & Hale, M. (2023). Differential privacy for symbolic systems with application to Markov Chains. *Automatica*, 152, 110908.

[29] Huo, X., & Liu, M. (2021). Privacy-preserving distributed multi-agent cooperative optimization-paradigm design and privacy analysis. *IEEE Control Systems Letters*, 6, 824-829.

[30] Farokhi, F., & Esfahani, P. M. (2018, December). Security versus privacy. *In 2018 IEEE Conference on Decision and Control (CDC)* (pp. 7101-7106). IEEE.

[31] Chong, M. S., Sandberg, H., & Teixeira, A. M. (2019, June). A tutorial introduction to security and privacy for cyber-physical systems. *In 2019 18th European Control Conference (ECC)* (pp. 968-978). IEEE.

[32] Liu, S., Trivedi, A., Yin, X., & Zamani, M. (2022). Secure-by-construction synthesis of cyber-physical systems. *Annual Reviews in Control*, 53, 30-50.

[33] Ding, D., Han, Q.L., Xiang, Y., Ge, X., & Zhang, X. M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 275, 1674-1683.

[34] Weerakkody, S., Ozel, O., Mo, Y., & Sinopoli, B. (2019). Resilient control in cyber-physical systems: Countering uncertainty, constraints, and adversarial behavior. *Foundations and Trends® in Systems and Control*, 7(1-2), 1-252.

[35] Kordestani, M., & Saif, M. (2021). Observer-based attack detection and mitigation for cyberphysical systems: A review. *IEEE Systems, Man, and Cybernetics Magazine*, 7(2), 35-60.

[36] Duo, W., Zhou, M., & Abusorrah, A. (2022). A survey of cyber-attacks on cyber physical systems: Recent advances and challenges. *IEEE/CAA Journal of Automatica Sinica*, 9(5), 784-800.

[37] Burbano, L., Garg, K., Leudo, S. J., Cardenas, A.

[50] Farokhi, F., Shames, I., & Batterham, N. (2017). Secure and private control using semi-homomorphic encryption. *Control Engineering Practice*, 67, 13-20.

[51] Kogiso, K. & Fujita, T. (2015, December). Cyber-security enhancement of networked control systems using homomorphic encryption. In *2015 54th IEEE Conference on Decision and Control (CDC)*, (pp. 6836-6843).

[52] Teranishi, K., Shimada, N., & Kogiso, K. (2020). Stability-guaranteed dynamic ElGamal cryptosystem for encrypted control systems. *IET Control Theory & Applications*, 14(16), 2242-2252.

[53] Farokhi, F., Shames, I., & Batterham, N. (2016). Secure and private cloud-based control using semi-homomorphic encryption. *IFAC-PapersOnLine*, 49(22), 163-168.

[54] Darup, M.S. (2020). Encrypted polynomial control based on tailored two-party computation. *International Journal of Robust and Nonlinear Control*, 30(11), 4168-4187.

[55] Schlor, S., Hertneck, M., Wildhagen, S., & Allgöwer, F. (2021, December). Multi-party computation enables secure polynomial control based solely on secret-sharing. *In 2021 60th IEEE conference on decision and control (CDC)* (pp. 4882-4887). IEEE.

[56] Murguia, C., Farokhi, F., & Shames, I. (2020). Secure and private implementation of dynamic controllers using semihomomorphic encryption. *IEEE Transactions on Automatic Control*, 65(9), 3950-3957.

[57] Cheon, J. H., Han, K., Kim, H., Kim, J., & Shim, H. (2018, December). Need for controllers having integer coefficients in homomorphically encrypted dynamic system. *In 2018 IEEE Conference on Decision and Control (CDC) (pp. 5020-5025)*. IEEE.

[58] Schlüter, N., & Darup, M. S. (2021). On the stability of linear dynamic controllers with integer coefficients. *IEEE Transactions on Automatic Control*, 67(10), 5610-5613.

[59] Tavazoei, M.S. (2022). Non-minimality of the realizations and possessing state matrices with integer elements in linear discrete-time controllers. *IEEE Transactions on Automatic Control*, 68(6), 3698-3703.

[60] Tavazoei, M.S. (2023). Pisot number-based discrete-time controllers with integer state matrices to ensure monotonic closed-loop step responses. *IEEE Transactions on Automatic Control*, In press.

[61] Kim, J., Shim, H., & Han, K. (2022). Dynamic controller that operates over homomorphically encrypted data for infinite time horizon. *IEEE Transactions on Automatic Control*, 68(2), 660-672.

[62] Darup, M.S., Redder, A., Shames, I., Farokhi, F., & Quevedo, D. (2017). Towards encrypted MPC for linear constrained systems. *IEEE Control Systems Letters*, 2(2), 195-200.

[63] Schlüter, N. & Darup, M.S. (2020, December). Encrypted explicit MPC based on two-party computation and convex controller decomposition. In *2020 59th IEEE Conference on Decision and Control (CDC)*, 5469-5476.

[64] Alexandru, A.B., Morari, M., & Pappas, G.J. (2018, December). Cloud-based MPC with encrypted data. In *2018 IEEE Conference on Decision and Control (CDC)*, 5014-5019.

[65] Darup, M. S., Redder, A., & Quevedo, D. E. (2018). Encrypted cloud-based MPC for linear systems with input constraints. *IFAC-PapersOnLine*, 51(20), 535-542.

[66] Darup, M. S. (2020). Encrypted MPC based on ADMM real-time iterations. *IFAC-PapersOnLine*, 53(2), 3508-3514.

[67] Alexandru, A.B., Gatsis, K., Shoukry, Y., Seshia, S.A., Tabuada, P., & Pappas, G.J. (2020). Cloud-based quadratic optimization with partially homomorphic encryption. *IEEE Transactions on Automatic Control*, 66(5), 2357-2364.

[68] Zhang, Z., Che, X., Jiao, X., Yu, W., & Wan, L. (2022, May). Quadratic Optimization Using Additive Homomorphic Encryption in CPS. In *2022 13th Asian Control Conference (ASCC)* (pp. 1995-2000). IEEE.

[69] Yang, Z., Zhang, Z., & Tian, Y. (2022, May). Experimental Validation of Encrypted Quadratic Optimization Implemented on Raspberry Pi. In *2022 13th Asian Control Conference (ASCC)* (pp. 2018-2023). IEEE.

[70] Adelipour, S. & Haeri, M. (2023, May) Privacy-preserving model predictive control using secure multi-party computation, In *2023 31st International Conference on Electrical Engineering (ICEE)* (pp. 915-919). IEEE.

[71] Tjell, K., & Wisniewski, R. (2019, December). Privacy preservation in distributed optimization via dual decomposition and ADMM. *In 2019 IEEE 58th Conference on Decision and Control (CDC)* (pp. 7203-7208). IEEE.

[72] Tian, N., Guo, Q., Sun, H., & Zhou, X. (2022). Fully privacy-preserving distributed optimization in power systems based on secret sharing. *Energy*, 1(3), 351-362.

[73] Hossein ali zadeh, T., Turkmen, F., & Monshizadeh, N. (2022). Private computation of polynomials over networks. *Systems & Control Letters*, 166, 105291.

[74] Tjell, K. & Wisniewski, R. (2020). Privacy preserving distributed summation in a connected graph. *IFAC-PapersOnLine*, 53(2), 3445-3450.

Matschinske, J., & Baumbach, J. (2022). Privacy-preserving artificial intelligence techniques in biomedicine. *Methods of Information in Medicine*, 61, e12-e27.

[89] Weng, H., Hettiarachchi, C., Nolan, C., Suominen, H., & Lenskiy, A. (2023). Ensuring security of artificial pancreas device system using homomorphic encryption. *Biomedical Signal Processing and Control*, 79, 104044.

[90] Ying, Z., Cao, S., Liu, X., Ma, Z., Ma, J., & Deng, R. H. (2022). PrivacySignal: Privacy-preserving traffic signal control for intelligent transportation system. *IEEE Transactions on Intelligent Transportation Systems*, 23(9), 16290-16303.

[91] Kang, H.E.D., Kim, D., Kim, S., Kim, D.D., Cheon, J.H., & Anthony, B.W. (2021). Homomorphic encryption as a secure PHM outsourcing solution for small and medium manufacturing enterprise. *Journal of Manufacturing Systems*, 61, 856-865.

[92] Kogiso, K. (2018, December). Attack detection and prevention for encrypted control systems by application of switching-key management. In *2018 IEEE Conference on Decision and Control (CDC)*, (pp. 5032-5037).

[93] Kawano, Y., Kashima, K., & Cao, M. (2021). Modular control under privacy protection: Fundamental trade-offs. *Automatica*, 127, 109518.

[94] Kogiso, K. (2018, June). Upper-bound analysis of performance degradation in encrypted control system. In *2018 Annual American Control Conference (ACC)*, (pp. 1250-1255).

[95] Teranishi, K. & Kogiso, K. (2021). ElGamal-type encryption for optimal dynamic quantizer in encrypted control systems. *SICE Journal of Control, Measurement, and System Integration*, 14(1), 59-66.

[96] Soleymani, M., Mahdavifar, H., & Avestimehr, A. S. (2022). Analog secret sharing with applications to private distributed learning. *IEEE Transactions on Information Forensics and Security*, 17, 1893-1904.

[97] Teranishi, K., Ueda, J., & Kogiso, K. (2020). Event-triggered approach to increasing sampling period of encrypted control systems. *IFAC-PapersOnLine*, 53(2), 3502-3507.

[98] Damgård, I., Geisler, M., Krøigaard, M., & Nielsen, J. B. (2009, March). Asynchronous multiparty computation: Theory and implementation. *In International workshop on public key cryptography* (pp. 160-179). Berlin, Heidelberg: Springer.

[99] Fauser, M., & Zhang, P. (2021, December). Resilient homomorphic encryption scheme for cyber-physical systems. *In 2021 60th IEEE Conference on Decision and Control (CDC)* (pp. 5634-5639). IEEE.

[75] Darup, M.S., Redder, A., & Quevedo, D.E. (2018). Encrypted cooperative control based on structured feedback. *IEEE control systems letters*, 3(1), 37-42.

[76] Lu, Y., & Zhu, M. (2018). Privacy preserving distributed optimization using homomorphic encryption. *Automatica*, 96, 314-325.

[77] Wu, T., Zhao, C., & Zhang, Y.J.A. (2021). Privacy-preserving distributed optimal power flow with partially homomorphic encryption. *IEEE Transactions on Smart Grid*, 12(5), 4506-4521.

[78] Huo, X. & Liu, M. (2022). Distributed privacy-preserving electric vehicle charging control based on secret sharing. *Electric Power Systems Research*, 211, 108357.

[85] Fang, W., Zamani, M., & Chen, Z. (2021). Secure and privacy preserving consensus for second-order systems based on Paillier encryption. *Systems & Control Letters*, 148, 104869.

[86] Zhang, Z., Cheng, P., Wu, J., & Chen, J. (2020). Secure State Estimation Using Hybrid Homomorphic Encryption Scheme. *IEEE Transactions on Control Systems Technology*, 29(4), 1704-1720.

[81] Sadeghikhorami, L., Zamani, M., Chen, Z., & Safavi, A.A. (2020). A secure control mechanism for network environments. *Journal of the Franklin Institute*, 357(17), 12264-12280.

[82] Sadeghikhorami, L., Varadharajan, V., & Safavi, A.A. (2021). A novel secure observer-based controller and attack detection scheme for Networked Control Systems. *Information Sciences*, 575, 185-205.

[83] Sadeghikhorami, L. & Safavi, A.A. (2021). Secure distributed Kalman filter using partially homomorphic encryption. *Journal of the Franklin Institute*, 358(5), 2801-2825.

[84] Alanwar, A., Gassmann, V., He, X., Said, H., Sandberg, H., Johansson, K.H., & Althoff, M. (2023). Privacy-preserving set-based estimation using partially homomorphic encryption. *European Journal of Control*, 71, 100786.

[85] Feng, Z., Cao, G., Grigoriadis, K.M., & Pan, Q. (2023). Secure MPC-based Path-Following for UAS in Adverse Network Environment. *IEEE Transactions on Industrial Informatics*, In press.

[86] Solnør, P., Petrovic, S., & Fossen, T. I. (2023). Towards Oblivious Guidance Systems for Autonomous Vehicles. *IEEE Transactions on Vehicular Technology*, 72(6), 7067-7081.

[87] Hassija, V., Chamola, V., Bajpai, B.C., & Zeadally, S. (2021). Security issues in implantable medical devices: Fact or fiction?. *Sustainable Cities and Society*, 66, 102552.

[88] Torkzadehmahani, R., Nasirigerdeh, R., Blumenthal, D.B., Kacprowski, T., List, M.,

[100] Fauser, M., & Zhang, P. (2022, June). Detection of cyber-attacks in encrypted control systems. *In 2022 American Control Conference (ACC)* (pp. 4992-4997). IEEE.

[101] Miyamoto, M., Teranishi, K., Emura, K., & Kogiso, K. (2023). Cybersecurity-Enhanced Encrypted Control System Using Keyed-Homomorphic Public Key Encryption. *IEEE Access*, 11, 45749-45760.

[102] Naseri, A.M., Lucia, W., & Youssef, A. (2023). Confidentiality attacks against encrypted control systems. *Cyber-Physical Systems*, 9(3), 224-243.