# Enhanced Cybersecurity for Networked Motion Control Systems with Somewhat Homomorphic Encryption

---

**Encryption for motion control systems is very limited**

Cybersecurity of networked automation systems is an emerging field of research, with little study of protection for motion control systems. While encryption effectively secures data by encapsulating sensitive information at the communication level, when applied to motion control systems, the increasing multiplicative depth creates overflow (meaning the cipher text can no longer be decrypted back to plain text) and leads to loss of precision and loss of protection.

**Rewrite rules reduce the depth of encryption and improve numeric stability**

Expression rewrite rules for encrypted dynamic control schemes reduce the multiplicative depth of somewhat homomorphic encryption and improve numerical stability, translating to increased cybersecurity. This new approach encrypts motion control algorithms, sensor signals, model parameters, feedback and feedforward gains, and performs necessary computation in the ciphertext space to generate motion commands to servo systems without creating a security hole. Information decryption and control signal calculation can be performed and executed inside the plant, but all sensitive system information outside of the plant is always encrypted.

The topological sorting of algorithms based on associative rewrite rules effectively addresses potential overflow issues.

**Summary Bullets**

- Increase cybersecurity with expression rewrite rules for encrypted dynamic control schemes that reduce the multiplicative depth of somewhat homomorphic encryption and improve numerical stability.
- New approach generates motion commands to servo systems without creating a security hole.
- Information decryption and control signal calculation can be performed and executed inside the plant, while all sensitive system information outside of the plant is always encrypted.

Solution Advantages

- **Enhanced security**: Homomorphic encryption makes it possible to perform calculations on encrypted data, ensuring protection both inside and outside of the plant
- **Tested**: The expression rewrite rules reduced the depth from 6 to 4 in the encryption of a computed torque control scheme (also, termed as feedback linearization) of a planar revolute-prismatic manipulator
- **Reduces computing time**: Cuts depth of expression by one third, decreasing computing time
- **Robust**: Enables encryption for more complicated mechanical control systems
- **Increased Compatibility**: Rewrites translate expressions to be more compatible with leveled homomorphic schemes such as (BFV, BGV, CKKS, etc.)

Potential Commercial Applications

- Cybersecurity and protection for networked motion-control systems
- Secure control of robotic systems
- Privacy-preserved remote health monitoring and automated early diagnostic systems
- Secure processing of sensitive information
- Cyber physical systems
- Networked manufacturing and assembly
- Autonomous vehicles

**Inventors**


- Dr. Jun Ueda
  Professor - Georgia Tech School of Mechanical Engineering
- Shane Kosieradzki
  Graduate Research Assistant - Georgia Tech Research Institute

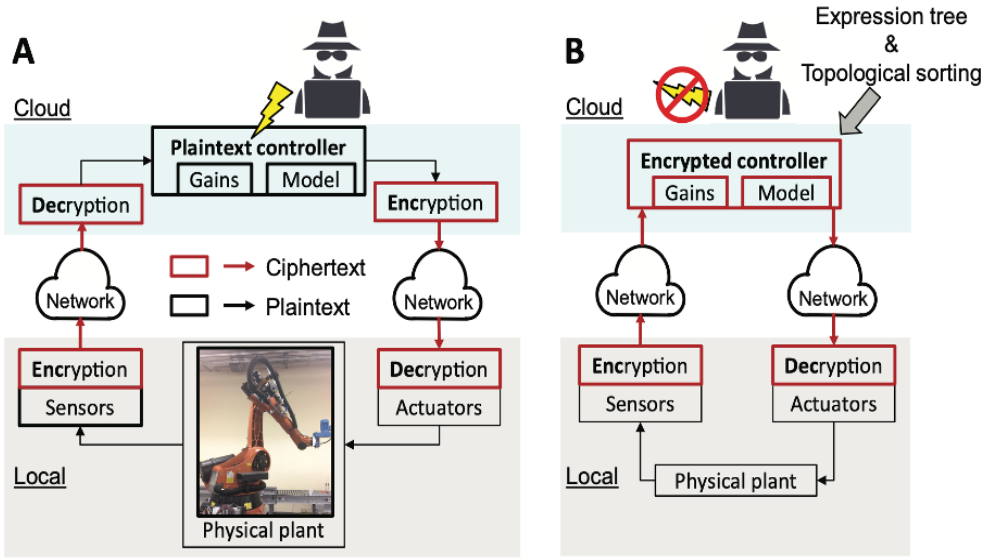

**IP Status**

Patent application has been filed : US63/368075

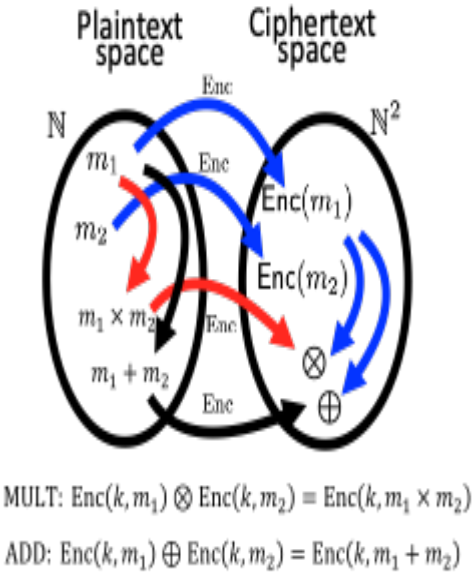
**Publications**


Rewrite Rules for Automated Depth Reduction of Encrypted Control Expressions with Somewhat Homomorphic Encryption, IEEE/ASME (AIM) International Conference on Advanced Intelligent Mechatronics - July 11, 2022


**Images**



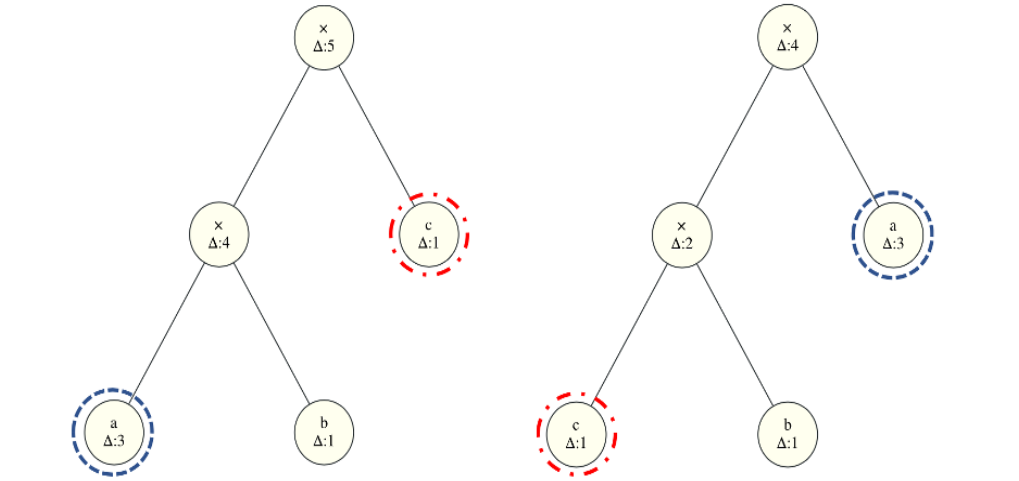

Security-enhanced networked control. A) Conventional encrypted communication (control scheme computation in plaintext), B) Encrypted control (control scheme computation in ciphertext)




$$\text{MULT: } \mathrm{Enc}(k, m_1) \otimes \mathrm{Enc}(k, m_2) = \mathrm{Enc}(k, m_1 \times m_2)$$

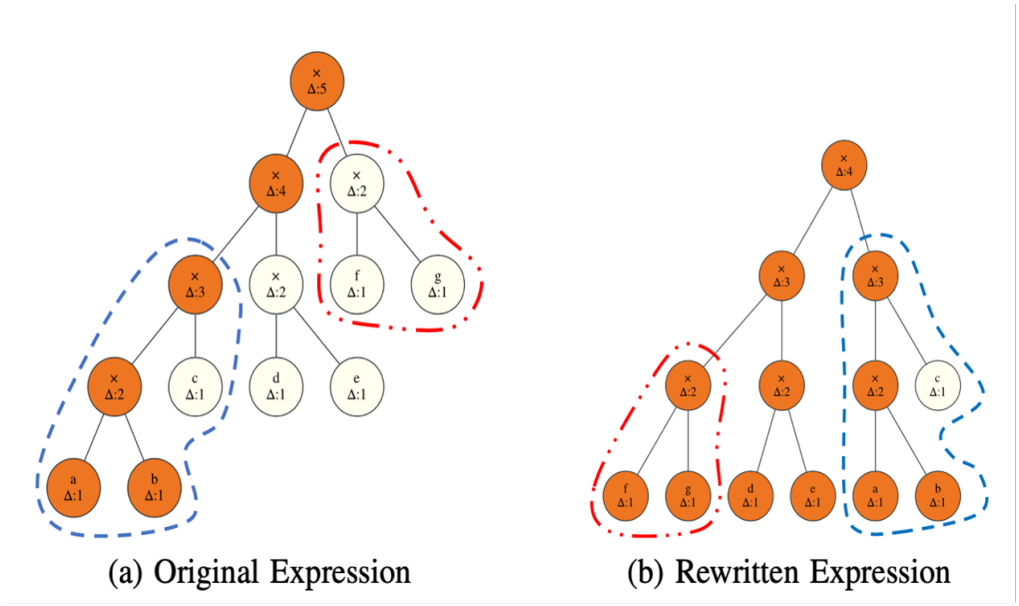
$$\text{ADD: } \mathrm{Enc}(k, m_1) \oplus \mathrm{Enc}(k, m_2) = \mathrm{Enc}(k, m_1 + m_2)$$

Somewhat Homomorphic encryption (SHE)



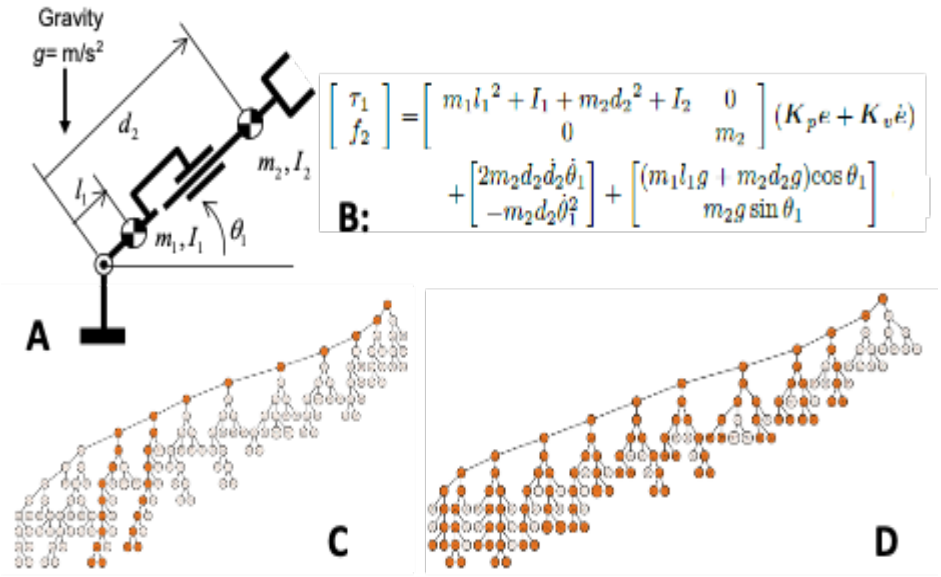

(a) Original (b) Rewritten

The left expression has a node of greater depth, “a,” deeper in the tree. By swapping with “a” shallower node, “c,” node “a” is lifted up, and the total depth is reduced by one.




(a) Original Expression (b) Rewritten Expression

On the left is the original expression. On the right is the output of the associative rewrite. The circled regions have been swapped with each other in the rewritten circuit. The depth is reduced by one.




By utilizing the proposed rewrites, control expressions (B) of a dynamic system (A) can be transformed from a non-optimal format (C) to a format more compatible with leveled homomorphic cyphers (D)

Visit the Technology here:
Enhanced Cybersecurity for Networked Motion Control Systems with Somewhat Homomorphic Encryption

---