Toward Nonlinear Dynamic Control over Encrypted Data for Infinite Time Horizon ⋆

Junsoo Kim * **Farhad Farokhi** ** **Iman Shames** **
Hyungbo Shim *

* ASRI, Dep. of Electrical and Computer Engineering, Seoul National University, Seoul, Korea.
** Dep. of Electrical and Electronic Engineering, The University of Melbourne, Parkville, VIC 3010, Australia.

Abstract: Recent studies on encrypted control using homomorphic encryption allow secure operation by directly performing computations on encrypted data without decryption. Implementing dynamic controllers on encrypted data presents unique challenges due to limitations on the number of operations on an encrypted message. Hence, it may not be possible to perform the recursive operations for an infinite time horizon. In this note, we demonstrate that it is possible to run a dynamic controller over encrypted data for an infinite time horizon if the output of the controller can be represented as a function of a fixed number of previous inputs and outputs. The presented implementation requires encryption at both input and output of the plant. We identify a class of nonlinear systems that can accommodate the proposed implementation. The closed-loop performance can be guaranteed using the proposed encrypted controller by ensuring that quantization error is made arbitrarily small with appropriate choice of parameters. We show that the proposed method is amenable to linear systems (as a subset of the said nonlinear systems) with performance guarantees.

Keywords: Secure networked control systems, Privacy, Security, Control over networks, Control over encrypted data.

1. ENCRYPTED CONTROL

The notion of encrypted control, introduced by Kogiso and Fujita (2015), Farokhi et al. (2017), and Kim et al. (2016), aims for security enhancement by performing all the operations in networked controllers directly over encrypted data without decryption.

Let a simple form of static controller be given as

$$u(t) = h(y(t)), \quad t = 0, 1, 2, \cdots,$$

where $y(t) \in \mathbb{R}^p$ is the input of the controller (the output of the plant), and $u(t) \in \mathbb{R}$ is the output of the controller (the input of the plant). And, suppose that it is implemented in a digital computer as

$$\overline{u}(t) = \overline{h}\left(\left\lceil \frac{y(t)}{r} \right\rfloor\right) =: \overline{h}(\overline{y}(t)) \in \mathbb{Z}_N, \quad (1a)$$

$$u_q(t) = \mathsf{L} \cdot \overline{u}(t), \quad (1b)$$

in which $\mathbb{Z}_N := \{i \in \mathbb{Z} : -N/2 \le i < N/2\}$ denotes the set of integers from $-N/2$ to $N/2$ with $N \in \mathbb{N}$ chosen sufficiently large, $\lceil \cdot \rfloor$ is the (component-wise) rounding operation, $\mathsf{r} > 0$ is the step size for quantization of $y(t) \in \mathbb{R}^p$ so that the components of $\overline{y}(t) = \lceil y(t)/\mathsf{r} \rfloor$ are all integers, $\overline{h}(\cdot)$ is a function consisting of additions or multiplications so that it results in $\overline{u}(t) \in \mathbb{Z}_N$, and $\mathsf{L} > 0$

is a scale factor so that the real-valued output $u_q(t) \in \mathbb{R}$, which is approximate to $u(t)$, is obtained from $\overline{u}(t)$.

The realization of encrypted control is possible when the employed cryptosystem allows arithmetic operations over encrypted data. For a vector of integers in $\mathbb{Z}_N$, let $\mathsf{Enc}(\cdot, \mathsf{sk})$ be the encryption algorithm with secret key sk (or a public key) so that $\mathsf{Enc}(m, \mathsf{sk})$ is an encrypted message of a vector $m \in \mathbb{Z}_N^p$, $\mathsf{p} \ge 1$, and $\mathsf{Dec}(\cdot, \mathsf{sk})$ be the decryption algorithm satisfying $\mathsf{Dec}(\mathsf{Enc}(m, \mathsf{sk}), \mathsf{sk}) = m$, $\forall m \in \mathbb{Z}_N^p$. Suppose that the encryption Enc is _homomorphic_ with respect to the function $\overline{h}$, i.e., there exists an operation $\mathbf{h}(\cdot)$ over encrypted data such that it satisfies

$$\mathsf{Dec}(\mathbf{h}(\mathsf{Enc}(\overline{y}(t), \mathsf{sk})), \mathsf{sk}) = \overline{h}(\overline{y}(t))$$

for each message $\overline{y}(t)$ of integers. Then, the operation part (1a) can be implemented over encrypted data as

$$\mathbf{u}(t) = \mathbf{h}(\mathbf{y}(t)), \quad (2)$$

where $\mathbf{y}(t) := \mathsf{Enc}(\overline{y}(t), \mathsf{sk})$. Receiving the encrypted signal $\mathbf{y}(t)$ and yielding the output $\mathbf{u}(t)$ from which the real output $u_q(t)$ can be obtained by decryption as $u_q(t) = \mathsf{L} \cdot \mathsf{Dec}(\mathbf{u}(t), \mathsf{sk})$, it is clear that the performance of the encrypted controller (2) is the same with (1a), while it does not utilize the decryption or the secret key for the control operation part.

The elimination of secret key from the controller is significant in terms of security, so the concept of encrypted control has been considered in various applications, such

as model predictive control by Darup et al. (2018) or quadratic optimization by Shoukry et al. (2016).

In the meantime, *dynamic control* over encrypted data has been a challenge. Consider a dynamic controller written as

$$x(t + 1) = f(x(t), y(t)), \qquad t = 0, 1, 2, \cdots, \qquad (3)$$
$$u(t) = h(x(t)),$$

which additionally considers recursive update of the state $x(t) \in \mathbb{R}^n$. From the rationale that the controller (3) is supposed to stabilize the closed loop system with the plant, we assume that the norms of the signals $y(t)$, $x(t)$, and $u(t)$ are bounded by a known constant. One direct way for implementing (3) over encrypted data would be to design functions **f** and **h** over encrypted data so that they are equivalent to f and h, and have the encrypted state recursively updated for each time step, by the function **f**.

However, the recursive operation over encrypted data may not be possible for infinite time horizon because the number of operations that can be performed on ciphertexts may be limited. The related issues are as follows:

- The employed cryptosystem may not be "fully homomorphic," i.e., it may not be possible to implement all kinds of operations over encrypted data. For example, making the use of cryptosystems allowing additions only, it is known that the number of multiplications over encrypted data may be limited, especially when it considers multiplications with non-integer rational numbers. See (Cheon et al., 2018) for more details.
- Even if the employed cryptosystem is fully homomorphic so that all kinds of arithmetic operations can be performed infinite number of times in theory, it may not be feasible in practice, due to computational complexity. For example, the use of "bootstrapping" technique, developed by Gentry (2009), can be considered for the sake of both addition and multiplication unlimited number of times, but it may not be easily applied for control systems in practice, if the bootstrapping takes longer than the sampling period.

As a consequence, in terms of encrypted dynamic systems, most results in literature end up considering finite time dynamic operation (Alexandru et al., 2018; Murguia et al., 2021) or end up being satisfied with static operations over encrypted data (Darup et al., 2018).

2. TOWARD UNLIMITED DYNAMIC CONTROL

In this short note, we address that implementing the operation of (3) over encrypted data for infinite time horizon is rendered possible, if there exist an integer $\mathsf{m} \geq 1$ and a function g so that the system (3) can be represented as the form

$$\mathsf{u}(t) = g(\mathsf{u}(t-1), \cdots, \mathsf{u}(t-\mathsf{m}), y(t-1), \cdots, y(t-\mathsf{m})), \quad (4)$$

with the initial values $\{\mathsf{u}(-i)\}_{i=1}^{\mathsf{m}} \subset \mathbb{R}$ and $\{y(-i)\}_{i=1}^{\mathsf{m}} \subset \mathbb{R}^{\mathsf{p}}$, so that it satisfies $\mathsf{u}(t) = u(t)$ for all $t \geq 0$. To see the detail, let us consider encrypting (4); suppose that it is implemented over integers as

$$\overline{\mathsf{u}}'(t) = \overline{g}(\overline{\mathsf{u}}(t-1), \cdots, \overline{\mathsf{u}}(t-\mathsf{m}), \overline{y}(t-1), \cdots, \overline{y}(t-\mathsf{m})),$$

$$\mathsf{u}_q(t) = \mathsf{L} \cdot \overline{\mathsf{u}}'(t), \qquad \overline{\mathsf{u}}(t) = \left\lceil \frac{\mathsf{u}_q(t)}{\mathsf{r}} \right\rceil \qquad (5)$$

where $\overline{\mathsf{u}}(-i) = \lceil \mathsf{u}(-i)/\mathsf{r} \rceil$ and $\overline{y}(-i) = \lceil y(-i)/\mathsf{r} \rceil$, $i = 1, \cdots, \mathsf{m}$, are the initial values, $\overline{y}(t) = \lceil y(t)/\mathsf{r} \rceil$, $t \geq 0$, is the quantized input, the function $\overline{g}$ consisting of integer addition and multiplication yields the output $\overline{\mathsf{u}}'(t) \in \mathbb{Z}_N$ so that the approximate output $\mathsf{u}_q(t) \in \mathbb{R}$ is obtained by scaling with the factor $\mathsf{L} > 0$, and the output $\overline{\mathsf{u}}(t)$, as an integer of scale $1/\mathsf{r}$, is fed back to the controller at each time t.

Then, we suggest that the operation of (5) can be implemented over encrypted data to operate for infinite time horizon. In encrypted control systems, it is expected that the real-valued output $\mathsf{u}_q(t)$ would be obtained at the actuator with decryption, and it would be able to re-encrypt and transmit the encryption of $\overline{\mathsf{u}}(t)$ to the controller, as a newly encrypted message. As a result, it will be able to implement (5) over encrypted data as

$$\mathbf{u}(t) = \mathbf{g}\left(\{\mathsf{Enc}\left(\overline{\mathsf{u}}(t-i), \mathsf{sk}\right), \ \mathsf{Enc}\left(\overline{y}(t-i), \mathsf{sk}\right)\}_{i=1}^{\mathsf{m}} \right) \quad (6)$$

in which the encrypted controller receives both the signals $\overline{\mathsf{u}}(t)$ and $\overline{y}(t)$ as newly encrypted messages, and computes the function **g** over encrypted data which corresponds to the function $\overline{g}$ over integers. Then, the operation of (6) will not be recursive with respect to the number of operations for the encrypted messages, since the result $\mathbf{u}(t)$ will not be re-used for the operation, but to be transmitted to the actuator and decrypted. Hence, it is able to operate for infinite time horizon as long as the cryptosystem is homomorphic with respect to the function $\overline{g}$.

Finally, the following proposition suggests that the encrypted controller (6) can operate for infinite time horizon and its performance is the same with the quantized controller (5).

Proposition 1. Suppose that the encryption Enc is homomorphic with respect to the function $\overline{g}$. Then, the encrypted controller (6) can operate for infinite time horizon, i.e., it guarantees $\mathsf{L} \cdot \mathsf{Dec}(\mathbf{u}(t), \mathsf{sk}) = \mathsf{u}_q(t)$, for all $t \geq 0$. $\square$

Remark 2. Note that, in Proposition 1, the requirement for the employed cryptosystem is to be homomorphic for newly encrypted messages only (with respect to $\overline{g}$), rather than requiring that the encrypted messages can be used for the operation infinitely many times. In particular, there is no need of the use of bootstrapping techniques of fully homomorphic cryptosystems. $\square$

3. FURTHER ISSUES AND EXAMPLES

The proposed approach would be applicable when the given controller (3) can be converted to the form (4). In addition, we list several further issues that should be considered:

- For the conversion of (3) to the form (4) and (5), the function g should be found so that the performance of (4) should be equivalent to that of (3). And, in order to have the function $\overline{g}$ consist of additions and multiplications over integers, polynomial approximation methods should be considered for the function g, in practice.
- The effect of quantization errors. Considering that the closed loop of the plant and the given controller (3) is supposed to be stable with respect to external disturbances, such as the errors caused by quantization of signals, the converted controller (4) should satisfy

the same stability so that it can be implemented as (5) over quantized signals, in practice.

In the rest of this note, we suggest a class of nonlinear systems under which the above issues can be resolved. First, the following assumption asks that the given controller can be transformed into "observable canonical form".

Assumption 3. There exist $\mathsf{n}' \leq \mathsf{n}$ and a diffeomorphism $\Phi : \mathbb{R}^{\mathsf{n}} \to \mathbb{R}^{\mathsf{n}'} \times \mathbb{R}^{\mathsf{n}-\mathsf{n}'}$ such that, by $[z^{\top}, z'^{\top}]^{\top} := \Phi(x)$, the system (3) is transformed into the form

$$z(t+1) = \begin{bmatrix} z_1(t+1) \\ z_2(t+1) \\ z_3(t+1) \\ \vdots \\ z_{\mathsf{n}'}(t+1) \end{bmatrix} = \begin{bmatrix} g_1(z_{\mathsf{n}'}(t), y(t)) \\ g_2(z_1(t), z_{\mathsf{n}'}(t), y(t)) \\ g_3(z_1(t), z_2(t), z_{\mathsf{n}'}(t), y(t)) \\ \vdots \\ g_{\mathsf{n}'}(z(t), y(t)) \end{bmatrix}$$

$$z'(t+1) = g'(z(t), z'(t), y(t)) \tag{7}$$

$$u(t) = z_{\mathsf{n}'}(t).$$

□

Then, the following proposition states that the system (7) can be implemented as the form (4), with the same performance.

Proposition 4. Under Assumption 3, there exists a function g with $\mathsf{m} = \mathsf{n}'$, such that the operations of (4) and (7) are identical, i.e., it satisfies $\mathsf{u}(t) = u(t)$, $\forall t \geq 0$. □

Moreover, the following corollary suggests that the system (7) can be implemented over integers and quantized signals as in (5), when the functions $\{g_i\}_{i=1}^{\mathsf{n}'}$ are of real polynomials (or able to be approximated with real polynomials), where the performance error due to quantization can be made arbitrarily small with the choice of parameters. And then, according to Proposition 1, it will be able to be implemented over encrypted data with the same performance as well, and able to operate for infinite time horizon without decryption.

Corollary 5. Suppose that Assumption 3 holds, and the functions $\{g_i\}_{i=1}^{\mathsf{n}'}$ are of real polynomials. Then, for every $\epsilon > 0$, there exist $\mathsf{r}' > 0$, $\mathsf{L}' > 0$, and a polynomial $\bar{g}$ of integer coefficients such that for every $\mathsf{r} < \mathsf{r}'$ and $\mathsf{L} < \mathsf{L}'$, the quantized controller (5) guarantees $\|\mathsf{u}_q(t) - u(t)\| < \epsilon$, for all $t \geq 0$. Furthermore, the encrypted controller (6) guarantees

$$\|\mathsf{L} \cdot \mathsf{Dec}(\mathbf{u}(t), \mathsf{sk}) - u(t)\| < \epsilon,$$

for all $t \geq 0$. □

Finally, the following proposition suggests that every linear system satisfies the condition of Assumption 3, so that the proposed method is applicable for all linear systems.

Proposition 6. Given the system (3), suppose that f and h are of linear functions. Then, there exists an invertible matrix $T \in \mathbb{R}^{\mathsf{n} \times \mathsf{n}}$ such that, by $[z^{\top}, z'^{\top}]^{\top} = Tx$, the system (3) is transformed into the form (7), where $\{g_i\}_{i=1}^{\mathsf{n}'}$ and g' are of linear functions. □

Remark 7. From the combination of Corollary 5 and Proposition 6, it is clear that all linear systems can be encrypted to operate for infinite time horizon, in which the performance error due to quantization can be made arbitrary small. It accords with the previous result in Kim et al. (2019), but it should be noted that the results of this paper based on Proposition 1 do not require that the encryption algorithm should be homomorphic for infinitely many times of operations (such as recursive operations). Instead, it requires the cryptosystem to be homomorphic only for finitely many additions or multiplications. □

4. CONCLUSION

In this short note, we have reviewed the challenge of implementing dynamic controllers over encrypted data in terms of operating for infinite time horizon. Considering that the output of the encrypted controller is supposed to be decrypted at the actuator so that it would be able to be re-encrypted and transmitted the the controller again, we suggest that dynamic control operations over encrypted data would be possible for infinite time horizon when the output of the system can be represented as a function of the previous inputs and outputs. Then, it is suggested that systems that are able to be represented as nonlinear observable canonical form can be implemented over encrypted data to operate for infinite time horizon, in which the performance error can be made arbitrarily small with the choice of parameters.

REFERENCES

Alexandru, A.B., Morari, M., and Pappas, G.J. (2018). Cloud-based MPC with encrypted data. In *Proceedings of 57th IEEE Conference on Decision and Control*, 5014–5019.

Cheon, J.H., Han, K., Kim, H., Kim, J., and Shim, H. (2018). Need for controllers having integer coefficients in homomorphically encrypted dynamic system. In *Proceedings of 57th IEEE Conference on Decision and Control*, 5020–5025.

Darup, M.S., Redder, A., Shames, I., Farokhi, F., and Quevedo, D.E. (2018). Towards encrypted MPC for linear constrained systems. *IEEE Control Systems Letters*, 2(2), 195–200.

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

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In *Proceedings of STOC*, volume 9, 169–178.

Kim, J., Lee, C., Shim, H., Cheon, J.H., Kim, A., Kim, M., and Song, Y. (2016). Encrypting controller using fully homomorphic encryption for security of cyber-physical systems. *IFAC-PapersOnline*, 49(22), 175–180.

Kim, J., Shim, H., and Han, K. (2019). Dynamic controller that operates over homomorphically encrypted data for infinite time horizon. ArXiv:1912.07362 [eess.SY].

Kogiso, K. and Fujita, T. (2015). Cyber-security enhancement of networked control systems using homomorphic encryption. In *Proceedings of 54th IEEE Conference on Decision and Control*, 6836–6843.

Murguia, C., Farokhi, F., and Shames, I. (2021). Secure and private implementation of dynamic controllers using semi-homomorphic encryption. *IEEE Transactions on Automatic Control*. In Press.

Shoukry, Y., Gatsis, K., Alanwar, A., Pappas, G.J., Seshia, S.A., Srivastava, M., and Tabuada, P. (2016). Privacy-aware quadratic optimization using partially homomorphic encryption. In *Proceedings of 55th IEEE Conference on Decision and Control*, 5053–5058.