

**Assistant Professor**, Department of Electrical and Information Engineering, Seoul National University of Science and Technology (SeoulTech), Korea

**Research interest: Control systems and security**

- Encrypted control system
- Homomorphic encryption
- Attack-resilient control
- Distributed protocols

E-mail        junsookim@seoultech.ac.kr  
                  junsookim4@gmail.com  
Homepage    <https://junsookim4.wordpress.com>  
Nationality   Korean

## Education

- 2014 – 2020    **M.S./Ph.D.**, Electrical and Computer Engineering,  
Seoul National University, Seoul, Korea  
Thesis title: *Homomorphic encryption of linear dynamic systems to operate for infinite time horizon*  
Supervisor: Prof. Hyungbo Shim
- 2009 – 2014    **B.S.**, Electrical and Computer Engineering & Mathematical Sciences (double major),  
Seoul National University, Seoul, Korea

## Work History

- 2022 – present    **Assistant Professor**, Department of Electrical and Information Engineering,  
Seoul National University of Science and Technology, Korea
- 2021 – 2022    **Postdoctoral Researcher**, Division of Decision and Control System,  
KTH Royal Institute of Technology, Sweden
- 2020 – 2021    **Postdoctoral Researcher**, Automation and Systems Research Institute (ASRI),  
Seoul National University, Seoul, Korea

## Honor, Awards, and Grants

Post-Doctoral Overseas Training Program, National Research Foundation of Korea, 2021-2022  
Distinguished Dissertation Award, Seoul National University, 2020

## Invited Talks

- Invited seminar**    at TU Dortmund, Germany, Mar. 24, 2022  
                          at the University of Seoul, Korea, Mar. 16, 2022  
                          at Seoul National University, Korea, Feb. 25, 2022  
                          at KTH Royal Institute of Technology, Sweden, Sep. 21, 2020  
                          at the University of Texas at Austin, United States, Aug. 29, 2020  
                          at the University of Melbourne, Australia, Feb. 7, 2020

**Invited speaker** at 13th Asian Control Conference, Jeju Island, Korea, May 4, 2022  
at ME Seminar, GIST, Korea, Apr. 14, 2022  
at 36th ICROS Conference, Yeosu, Korea, Jun. 23, 2021  
at 19th International Conference on Control, Automation and Systems,  
Jeju Island, Korea, Oct. 16, 2019  
at UT-SNU Joint Seminar in Electrical Engineering,  
Seoul National University, Korea, May 3, 2019  
at Conference on Math to Industry,  
Seoul National University, Korea, May 19, 2018

## Research & Teaching Experience

**Courses** (in SeoulTech) Engineering Mathematics 2, Fall 2022  
Signals and Systems, Fall 2022

**Visiting scholar** at TU Dortmund, Germany, Mar. 2022 (Prof. Moritz Schulze Darup)  
at the University of Melbourne, Australia, Feb. 2020 (Prof. Iman Shames)  
at the University of Electro-Communications, Japan, Nov. 2018 (Prof. Kiminao Kogiso)

## Professional Service

**Reviewer** IEEE Transactions of Automatic Control,  
Automatica,  
IEEE Transactions on Control of Network Systems,  
IEEE Transactions on Control Systems Technology,  
IEEE Transactions on Cybernetics,  
IET Control Theory & Applications,  
IEEE Control Systems Letters,  
IEEE Conference on Decision and Control,  
American Control Conference,  
European Control Conference,  
International Conference on Control, Automation and Systems

**Organizer / Chair** Organizer/Chair, "Encrypted Control and Optimization I/II,"  
IEEE Conference on Decision and Control (CDC), 2021  
Chair, "Network and Robot Applications,"  
International Conference on Control, Automation and Systems (ICCAS), 2020

## Publications

(\*: corresponding author)

**J. Kim**, D. Kim\*, Y. Song, H. Shim, H. Sandberg, and K. H. Johansson, "Comparison of encrypted control approaches and tutorial on dynamic systems using Learning With Errors-based homomorphic encryption," *Annual Reviews in Control*, accepted

R. Alisic\*, J. Kim, and H. Sandberg, "Model-free undetectable attacks on linear systems using LWE-based encryption," *IEEE Control Systems Letters*, under review

**J. Kim**, H. Shim\*, and K. Han, “Dynamic controller that operates over homomorphically encrypted data for infinite time horizon,” *IEEE Trans. on Automatic Control (Early Access)*, 2022

J. G. Lee and **J. Kim\***, “Mixed analog–digital method of designing a heterogeneous network with the desired collective behavior and rapid convergence,” *Systems and Control Letters*, vol. 160, no. 105126, 2022

J. G. Lee, **J. Kim**, and H. Shim\*, “Fully distributed resilient state estimation based on distributed median solver,” *IEEE Trans. on Automatic Control*, vol. 65, no. 9, pp. 3935–3942, 2020

**J. Kim**, C. Lee, H. Shim\*, Y. Eun, and J. H. Seo, “Detection of sensor attack and resilient state estimation for uniformly observable nonlinear systems having redundant sensors,” *IEEE Trans. on Automatic Control*, vol. 64, no. 3, pp. 1162–1169, 2019

J. H. Cheon, K. Han, S-M. Hong, H. J. Kim\*, **J. Kim**, S. Kim, H. Seo, H. Shim, and Y. Song, “Toward a secure drone system: flying with real-time homomorphic authenticated encryption,” *IEEE Access*, vol. 6, pp. 24325–24339, 2018

## Book chapter

**J. Kim**, H. Shim\*, and K. Han, “Comprehensive introduction to fully homomorphic encryption for dynamic feedback controller via LWE-based cryptosystem,” in *Privacy in Dynamical Systems*, Springer, Singapore, 2020

## Conference papers

**J. Kim\***, M. Schulze Darup, H. Sandberg, and K. H. Johansson, “Asymptotic stabilization over encrypted data with limited controller capacity and time-varying quantizer,” in *Proc. of 61th IEEE Conference on Decision and Control*, 2022, accepted

N. Schlüter\*, P. Binfet, **J. Kim**, and M. Schulze Darup, “Encrypted distributed state estimation via affine averaging,” in *Proc. of 61th IEEE Conference on Decision and Control*, 2022, under accepted

**J. Kim\***, H. Shim, H. Sandberg, and K. H. Johansson, “Method for running dynamic systems over encrypted data for infinite time horizon without bootstrapping and re-encryption,” in *Proc. of 60th IEEE Conference on Decision and Control*, 2021

M. Perez Chaher\*, B. Jayawardhana, and **J. Kim**, “Homomorphic encryption-enabled distance-based distributed formation control with distance mismatch estimators,” in *Proc. of 60th IEEE Conference on Decision and Control*, 2021

**J. Kim\***, H. Shim, and K. Han, “Design procedure for dynamic controllers based on LWE-based homomorphic encryption to operate for infinite time horizon,” in *Proc. of 59th IEEE Conference on Decision and Control*, 2020

D. Lee\*, **J. Kim**, and H. Shim, “Distributed aggregation over homomorphically encrypted data under switching networks,” in *Proc. of 59th IEEE Conference on Decision and Control*, 2020

J. H. Cheon\*, D. Kim, **J. Kim**, S. Lee, and H. Shim, “Authenticated computation of control signal from dynamic controllers,” in *Proc. of 59th IEEE Conference on Decision and Control*, 2020

J. Lee\*, **J. Kim**, and H. Shim, “Zero-dynamics attack on homomorphically encrypted control system,” in *Proc. of 20th International Conference on Control, Automation and Systems*, 2020

**J. Kim\*** and H. Shim, “Encrypted state estimation in networked control systems,” in *Proc. of 58th IEEE Conference on Decision and Control*, 2019

**J. Kim\***, J. G. Lee, C. Lee, H. Shim, and J. H. Seo, “Local identification of sensor attack and distributed resilient state estimation for linear systems,” in *Proc. of 57th IEEE Conference on Decision and Control*, 2018

J. H. Cheon, K. Han, H. Kim, **J. Kim**, and H. Shim\*, “Need for controllers having integer coefficients in homomorphically encrypted dynamic system,” in *Proc. of 57th IEEE Conference on Decision and Control*, 2018

**J. Kim\***, C. Lee, H. Shim, Y. Eun, and J. H. Seo, “Detection of sensor attack and resilient state estimation for uniformly observable nonlinear systems,” in *Proc. of 55th IEEE Conference on Decision and Control*, 2016

**J. Kim**, C. Lee, H. Shim\*, J. H. Cheon, A. Kim, M. Kim, and Y. Song, “Encrypting controller using fully homomorphic encryption for security of cyber-physical systems,” in *Proc. of 6th IFAC Workshop on Distributed Estimation and Control in Networked Systems*, 2016

## Patents

Method for processing dynamic data based on homomorphic encryption which carries out unlimited arithmetic operations without bootstrapping and re-encryption of control data

**J. Kim** and H. Shim

Korea Patent Application, 1020210006962, 2021,

PCT Application, PCT/KR2021/017080, 2021

Method for dynamic feedback control based on homomorphic encryption which carries out unlimited arithmetic operations without bootstrapping

H. Shim and **J. Kim**

Korea Patent Registration, 1020210042668, 2021,

PCT Application, PCT/KR2020/008097, 2020,

US Patent Application

Method for processing dynamic data by fully homomorphic encryption

H. Shim, J. H. Cheon, Y. Song, M. Kim, **J. Kim**, and C. Lee

Korea Patent Registration, 1020180092199, 2018,

PCT Application, PCT/KR2017/002479, 2018,

US Patent Registration, US10924262B2, 2021

## References

Name **Hyungbo Shim**  
University Seoul National University  
Position Professor (M.S. & Ph.D. supervisor)  
Contact hshim@snu.ac.kr

Name **Jin Heon Seo**  
University Seoul National University  
Position Professor (M.S. & Ph.D. co-supervisor)  
Contact jhseo@snu.ac.kr

Name **Karl H. Johansson**  
University KTH Royal Institute of Technology  
Position Professor (post-doc supervisor)  
Contact kallej@kth.se

Name **Henrik Sandberg**  
University KTH Royal Institute of Technology  
Position Professor (post-doc co-supervisor)  
Contact hsan@kth.se

Name **Jung Hee Cheon**  
University Seoul National University  
Position Professor (Ph.D. evaluation committee)

Contact    [jhcheon@snu.ac.kr](mailto:jhcheon@snu.ac.kr)