

# Integrating Levelled-Homomorphic Encryption in a Secure Process Control Application

Sebastian Leonow, Raphael Dyrska, Juraj Holaza, and Martin Mönnigmann

## Motivation & Goal

- Outsourcing computationally demanding controllers to a cloud reduces on-site hardware demand
- Homomorphic encryption allows to evaluate the control law on encrypted data without disclosing sensitive information
- We demonstrate control of a 1.1 kW water heater based on homomorphic encryption, using lean embedded hardware and a cloud computer

## Challenges

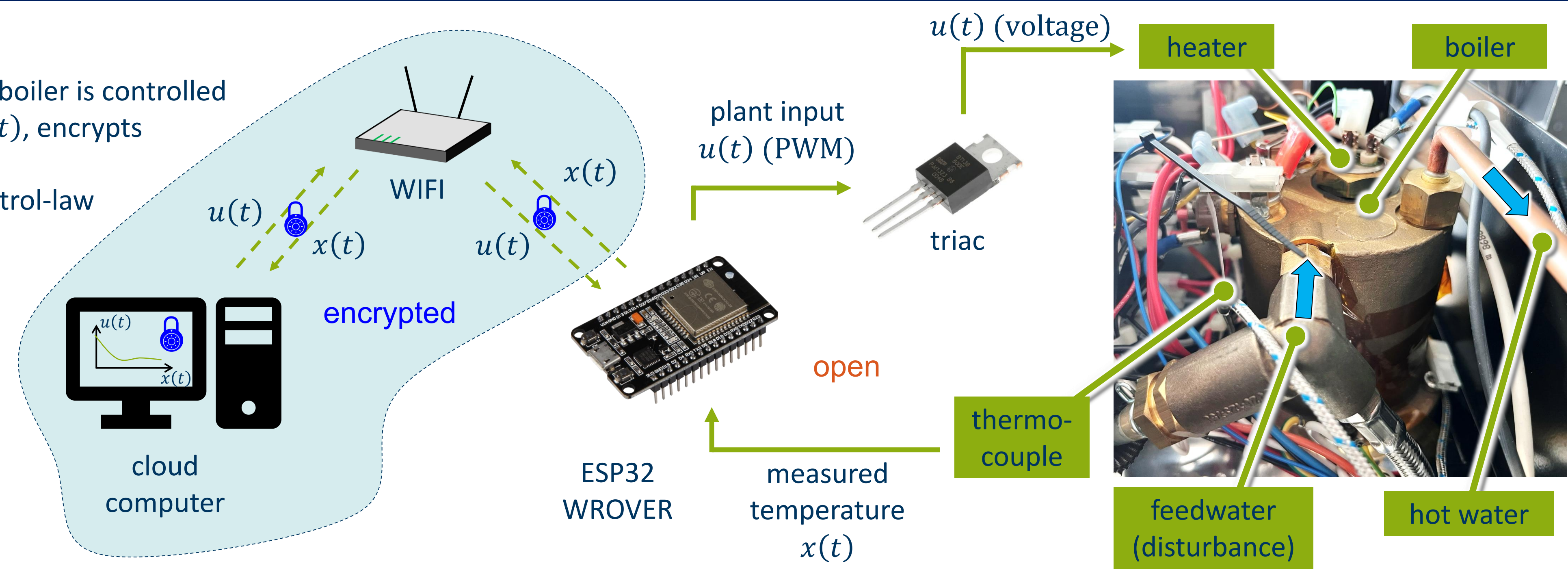
- Existing fully- or levelled-homomorphic encryption methods can handle even complex computations [1] but are computationally demanding
- Levelled-homomorphic methods are mature enough for transition into practical applications but have a limit on the number of subsequent mathematical operations
- On-site hardware shall be kept lean in computational power and energy demand

## Methods

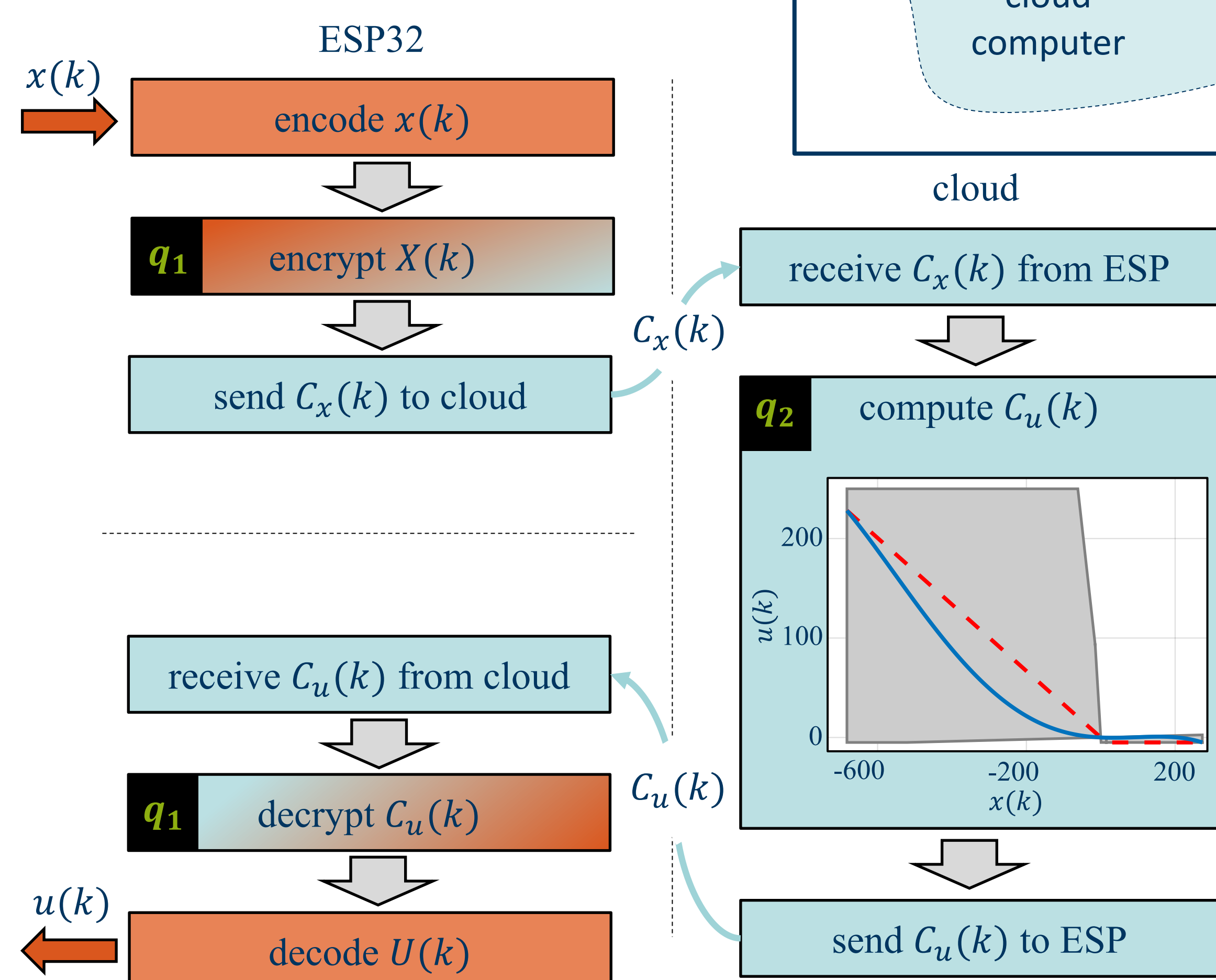
- We implement the levelled-homomorphic Brakerski Fan-Vercauteren (BFV) cryptosystem [2] and use Micropython as implementation language on an on-site ESP32 microcontroller
- We implement a polynomial control law approximating explicit model predictive control [3]
- We outline computational bottlenecks and optimize the specific computations to meet cycle time requirements

## Application setup

- The temperature of the hot water outflow from a boiler is controlled
- The ESP32 receives the measured temperature  $x(t)$ , encrypts it and sends it to the cloud
- The cloud computer evaluates the polynomial control-law and returns  $u(t)$  to the ESP32
- The cloud computer never decrypts any data
- The ESP32 decrypts  $u(t)$  and applies it to the heater



## Implementation



- The Brakerski Fan-Vercauteren cryptosystem works on dual  $N$ th-order polynomials representing plain- and ciphertexts, with integer coefficients modulo  $t$  for plaintext and modulo  $q_1$  for ciphertext
- Primary computational bottleneck is the convolution  $(*)$  of polynomials
- Number Theoretic Transform (NTT) representation allows element-wise multiplication of the polynomial coefficients, boosting convolution performance
- We extend NTT application also to the re-linearization after multiplication by switching to a larger modulus  $q_2 \sim q_1^n$ .
- Online- and pre-transformations further reduce the online computational load
- One cycle of closed-loop control with control law

$$u = (x^2 + k_1 x) \cdot (x^2 + k_2 x + k_3)$$

allows for the following online and pre-transformations (exemplary for the part  $k_1 x$ ):

Encryption of state  $X$  with pre-transformed public key  $P$  and online-transformed random  $U$ :

$$X_1' = [P' * U + \epsilon']_{q_1}, X_1' = [P' * U + \delta X + \epsilon']_{q_1}$$

Compute  $m_1 := k_1 x$  with modulus shift to  $q_2 = q_1^n$  for re-linearization after multiplication:

$$\text{rnd} \left( \frac{t \cdot ((X_1', K_1') * (K_1', X_2'))}{q_1} \right) \rightarrow \tilde{M}_1', \tilde{M}_1'', \tilde{M}_1''' ,$$

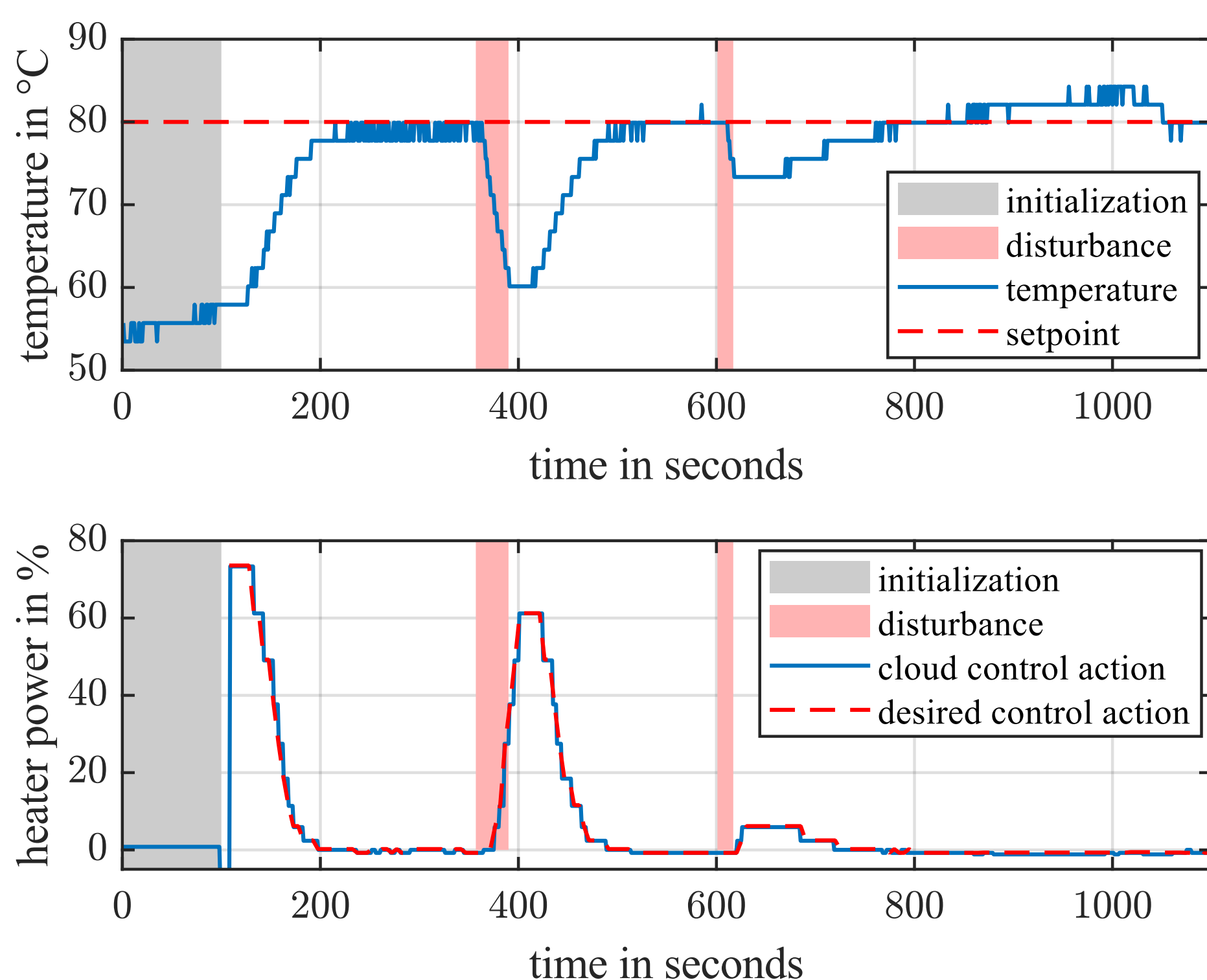
$$M_1' = \left[ \tilde{M}_1' + \text{rnd} \left( \frac{\tilde{M}_1''' * R'}{q_2} \right) \right]_{q_1}, M_1'' = \left[ \tilde{M}_1'' + \text{rnd} \left( \frac{\tilde{M}_1''' * R''}{q_2} \right) \right]_{q_1}$$

Decrypt control action  $U$ :

$$U = \left[ \frac{t \cdot \text{rnd}([M_1' + M_1'' * S]_{q_1})}{q_1} \right]_t$$

## Results

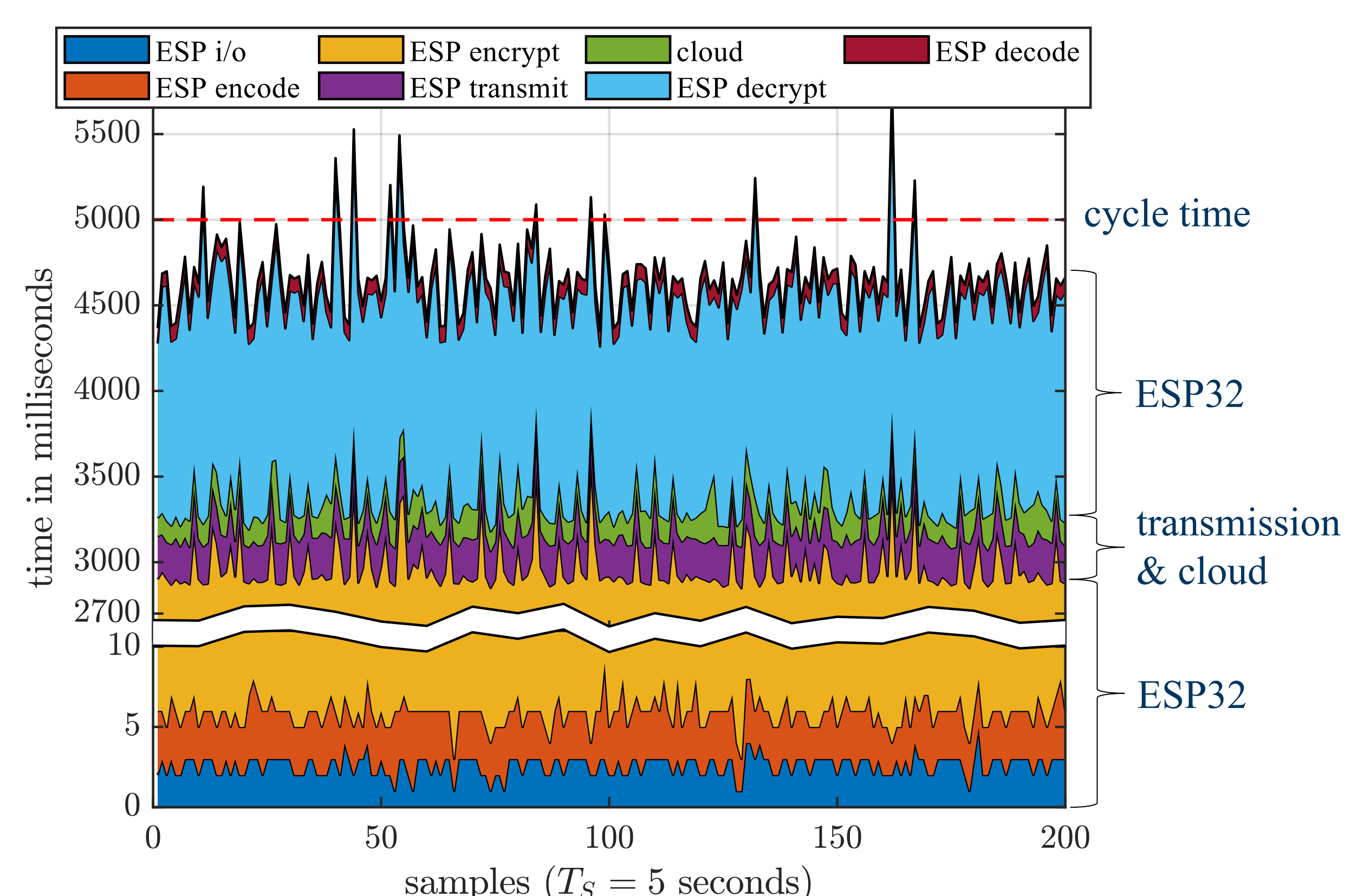
- We measured an approx. 15 minute time series of the closed-loop, secure control with fixed setpoint at 80°C and two disturbances by increased feedwater flow
- BFV parameters:  $N = 1024, t = 256, q_1 \sim 2^{51}, n = 4$ , cycle-time 5s



The encrypted control closely matches the unencrypted reference, demonstrating effective implementation.

The profiling reveals that encryption and decryption are most elaborate since they run on the slow ESP.

Controller evaluation (green) requires large number of time-consuming convolutions and takes up to 30 seconds when not optimized.



## References

- A. Bertolace et al. (2023). Homomorphically Encrypted Gradient Descent Algorithms for Quadratic Programming. 62nd IEEE Conference on Decision and Control, 3844-3849.
- J. Fan and F. Vercauteren (2012). Somewhat Practical Fully Homomorphic Encryption. Cryptology ePrint Archive.
- M. Kvasnica et al. (2011). Stabilizing Polynomial Approximation of Explicit MPC. Automatica 47 (10), 2292-2297.