FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

ASSIGNMENT OF BACHELOR'S THESIS

Title:	Timing side-channel attack on AES
Student:	Adam Zahumenský
Supervisor:	Ing. Jiří Buček, Ph.D.
Study Programme:	Informatics
Study Branch:	Computer Security and Information technology
Department:	Department of Computer Systems
Validity:	Until the end of summer semester 2019/20

Instructions

Study the topic of timing side-channel attacks of the AES cipher on modern CPUs with caches. Measure the times of a naive AES implementation and an AES implementation using T-boxes and analyze the dependence of the calculation time on data, key, and possibly other factors, and try to break the key. The final work will take the form of a laboratory exercise assignment for teaching in computer security subjects.

References

Will be provided by the supervisor.

prof. Ing. Pavel Tvrdík, CSc.
Head of Department

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
Dean

Prague February 14, 2019