# TITLE OF THE PAPER - IN ENGLISH

**Jan Wozniak**
Master Degree Programme (2), FIT BUT
E-mail: xwozni00@stud.fit.vutbr.cz

Supervised by: Peter Jurnečka
E-mail: ijurnecka@fit.vutbr.cz

**Abstract**: Encryption of real-time multimedia data transferes is one of the tasks for telecommunication infrastructure which should be considered in order to provide essential level of security. Execution time of ciphering algorithm could play fundamental role in delay of the packets, therefore, it provides interesting challenge in terms of optimization methods. This work focuses on paralellization possibilities of processing SRTP for the purposes of private gateway with the usage of OpenCL framework, utilization gateway‘s resources and analysis of potential improvement.

**Keywords**: AES, SRTP, general-purpose GPU, OpenCL, parallel computations, gateway, VoIP.

## 1 INTRODUCTION

One of the essential metrics for measuring VoIP Gateway performance is the number of simultaneous calls. It is affected mostly by the computational demands of used communication protocols and number of registered users. While the count of registered users provides very limited room for improvement by the nature of the problem itself, there could be wide variety of aproaches in implementing the protocol stacks.

Significant amount of resources are utilized during indirect simultaneous call sessions by processing multimedia packets. Since security has recently grown to be necessary feature in VoIP communication, and the encryption and decryption processes are designed with the idea of optimization, it is primary scope of interest of this work.

## 2 SRTP PROCESSING

Secure Real-time Transport Protocol was designed as an extension over RTP protocol to obtain security and confidentiality for multimedia sessions.

– packet consists of multiple independent blocks.

### 2.1 AES

– parallelization of computation of cells in AES block.

### 2.2 PERSISTENT THREAD

– larger kernels to minimize negative influence of startup execution of the kernel.

## 3 GATEWAY DESIGN

– integration of SRTP stack to the VoIP gateway.

## 4 CONCLUSION

– results of testing.

## REFERENCES