# REVIEW

of a foreign scientific consultant
on the dissertation work of Alisher Aliuly Skabylov
on the topic "Hardware and software for data encryption based on FPGA",
submitted for the degree of Doctor of Philosophy (PhD) in the specialty 8D06201 -
Radio engineering, electronics and telecommunications.

The dissertation work of A.A. Skabylov is devoted to the development of software and hardware for data protection during reception, transmission and signal processing. Methods of accelerating and improving data security have been applied. Electronic schemes for calculating multiplication modulo and their hardware implementation on FPGAs are proposed.

The first chapter provides an overview of the current state of the problem. The necessity of conducting research on this topic is indicated.

The second chapter presents the results of experimentally investigated generators of cryptographically stable pseudorandom sequences created on the basis of modern encryption algorithms. An encryption device has been developed and tested using FPGA based on NPSS. In the process of implementing this device, methods of multithreaded parallel computing with the formation of information modules based on a random number generator were applied.

On my recommendation, Skabylov A.A. completed a foreign scientific internship at the Lublin University of Technology, Polish People's Republic, under the guidance of Professor Waldemar Wojcik. During the internship, A.A. Skabylov received practical design skills, including participation in the study of methods for developing pseudorandom generators. He obtained experimental data on the statistical properties of the output sequences of the developed generators and confirmation of their compliance with the requirements.

The developed FPGA-based encryption device for high-speed data encryption can be integrated into personal computers, and with the hardware implementation of the block of a set of irreducible polynomials, as well as key generation and implementations of the encryption block with a conveyor organization, then autonomous high-performance encryption devices can be built on their basis.

The results of the dissertation work have been published in 4 papers, including 1 printed work published in an international peer-reviewed rating journal with a high impact factor, as well as presented at international and republican scientific conferences and seminars.

I believe that the dissertation work of Alisher Aliuly Skabylov satisfies all the requirements for the works submitted for the degree of Doctor of Philosophy (PhD)

and I recommend accepting the dissertation work of A.A. Skabylov for public defense for the degree of Doctor of Philosophy (PhD) under the educational program 8D06201 – Radio Engineering, electronics and telecommunications.

JONGTAE PARK

*Jongtae Park, Professor Emeritus*
*Kyungpook National University, Korea*
*Daegu, 41566 Korea*
*Email: jtpark@ee.knu.ac.kr*
*Phone: +82-10-9805-5543*

Декан

# ОТЗЫВ

**Зарубежного научного консультанта по диссертационной работе Алишера Алиулы Скабылова на тему "Аппаратное и программное обеспечение шифрования данных на основе ПЛИС", представленной на соискание ученой степени доктора философии (PhD) по специальности 8D06201 - радиотехника, электроника и телекоммуникации.**

Диссертационная работа А.А. Скабылова посвящена разработке программного и аппаратного обеспечения для защиты данных при приеме, передаче и обработке сигналов. Применены методы ускорения и повышения безопасности данных. Предлагаются электронные схемы для вычисления умножения по модулю и их аппаратная реализация на ПЛИС.

В первой главе дается обзор текущего состояния проблемы. Указывается на необходимость проведения исследований по данной теме.

Во второй главе представлены результаты экспериментального исследования генераторов криптографически устойчивых псевдослучайных последовательностей, созданных на основе современных алгоритмов шифрования. Разработано и протестировано устройство шифрования с использованием ПЛИС на базе NPSS. В процессе реализации данного устройства были применены методы многопоточных параллельных вычислений с формированием информационных модулей на основе генератора случайных чисел.

По моей рекомендации Скабылов А.А. прошел зарубежную научную стажировку в Люблинском технологическом университете Польской Народной Республики под руководством профессора Вальдемара Войчика. Во время стажировки А.А. Скабылов получил практические навыки проектирования, включая участие в изучении методов разработки псевдослучайных генераторов. Он получил экспериментальные данные о статистических свойствах выходных последовательностей разработанных генераторов и подтверждение их соответствия требованиям.

Разработанное шифрующее устройство на основе FPGA для высокоскоростного шифрования данных может быть интегрировано в персональные компьютеры, и при аппаратной реализации блока набора неприводимых многочленов, а также генерации ключей и реализации блока шифрования с конвейерной организацией, тогда могут быть созданы автономные высокопроизводительные устройства шифрования построенный на их основе.

Результаты диссертационной работы опубликованы в 4 статьях, в том числе в 1 печатной работе, опубликованной в международном рецензируемом рейтинговом журнале с высоким импакт-фактором, а также

представлены на международных и республиканских научных конференциях и семинарах.

Я считаю, что диссертационная работа Алишера Алиулы Скабылова удовлетворяет всем требованиям, предъявляемым к работам, представляемым на соискание ученой степени доктора философии (PhD), и рекомендую принять диссертационную работу А.А. Скабылова к публичной защите на соискание ученой степени доктора философии (PhD) по образовательной программе 8D06201 – Радиотехника, электроника и телекоммуникации.

/подпись имеется/
*Парк Чонтэ, профессор*
*Национальный университет Кенбук, Корея*
*Тэгу, 41566 Корея*
*Электронная почта: jtpark@ee.knu.ac.kr*
*Телефон: +82-10-9805-5543*

Университет логотипі

**«8D06201 – Радиотехника, электроника және телекоммуникациялар» мамандығы бойынша философия докторы (PhD) дәрежесін алу үшін Сқабылов Әлішер Әлиұлының «ПЛИС негізінде мәліметтерді шифрлауды аппараттық және бағдарламалық қамтамасыз ету» тақырыбы бойынша диссертациялық жұмысына шетелдік ғылыми жетекшісінің**

# ПІКІРІ

Ә. Ә. Сқабыловтың диссертациялық жұмысы сигналдарды қабылдау, тарату және өңдеу кезінде деректерді қорғауға арналған бағдарламалық және аппараттық құралдарды әзірлеуге арналған. Деректер қауіпсіздігін жеделдету және жақсарту әдістері қолданылды. Модульдік көбейту бойынша есептеуге арналған электрондық схемалар мен оларды ПЛИС-ке аппараттық енгізу ұсынылды.

Бірінші тарауда мәселенің ағымдағы күйіне шолу жасалады. Осы тақырып бойынша зерттеу жүргізу қажеттілігі көрсетілген.

Екінші тарауда заманауи шифрлау алгоритмдері негізінде жасалған криптографиялық тұрақты жалған кездейсоқ тізбектердің генераторларына эксперименттік зерттеу нәтижелері келтірілген. Позициялық емес көпмүшелік санау жүйесі негізіндегі ПЛИС көмегімен шифрлау құрылғысы әзірленді және сыналды. Бұл құрылғыны іске асыру барысында кездейсоқ сандар генераторы негізінде ақпараттық модульдерді құра отырып, көп ағынды параллельді есептеу әдістері қолданылды.

Менің ұсынысым бойынша Ә. Ә. Сқабылов профессор Вальдемар Войчиктің басшылығымен Польша Халық Республикасының, Люблин технологиялық университетінде шетелдік ғылыми тағылымдамадан өтті. Тағылымдама барысында Ә. Ә. Сқабылов жалған кездейсоқ генераторларды әзірлеу әдістерін зерттеуге қатысуды қоса алғанда, практикалық жобалау дағдыларын алды. Ол әзірленген генераторлардың шығыс тізбегінің статистикалық қасиеттері туралы эксперименттік мәліметтер алды және олардың сәйкестігін растады.

Жоғары жылдамдықты деректерді шифрлауға арналған ПЛИС-қа негізделген шифрлау құрылғысын дербес компьютерлерге біріктіруге болады, ал келтірілмейтін көпмүшелер жиынтығының блогын аппараттық түрде жүзеге асыру, сондай-ақ кілттерді құру және конвейерлік ұйыммен шифрлау блогын енгізу кезінде автономды жоғары өнімді шифрлау құрылғылары жасалуы мүмкін.

Диссертациялық жұмыстың нәтижелері 4 мақалада, оның ішінде импакт-факторы жоғары халықаралық рецензияланатын рейтингтік журналда жарияланған 1 баспа жұмысында жарияланды, сондай-ақ халықаралық және республикалық ғылыми конференциялар мен семинарларда ұсынылды.

Әлішер Әлиұлы Сқабыловтың диссертациялық жұмысы философия докторы (PhD) ғылыми дәрежесін алу үшін ұсынылатын жұмыстарға қойылатын барлық талаптарды қанағаттандырады деп санаймын және 8D06201 – Радиотехника, электроника және телекоммуникация білім беру бағдарламасы бойынша философия докторы (PhD) ғылыми дәрежесін алу үшін Ә.Ә. Сқабыловтың диссертациялық жұмысын көпшілік алдында қорғауға қабылдауды ұсынамын.

/қолы бар/

*Парк Чонтэ, профессор*
*Кенбук ұлттық университеті, Корея*
*Тэгу, 41566 Корея*
*Электрондық пошта: jtpark@ee.knu.ac.kr*
*Телефон: +82-10-9805-5543*