Сведения об официальном оппоненте по диссертации на соискание ученой степени кандидата технических наук Тихонова Сергея Владимировича «Исследование и разработка модификаций аппаратно-реализованных защитных блоковых преобразований, устойчивых к побочным атакам по цепям электропитания»

Фамилия Имя Отчество: *Молдовян Николай Андреевич*
Гражданство: *Россия*
Место основной работы:
организация: *Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН)*
почтовый адрес: *199178, Санкт-Петербург, 14-линия В.О., д. 39,*
телефон: *((812)) 328-51-85*
подразделение: *научно-исследовательский отдел проблем информационной безопасности*
должность: *заведующий лабораторией криптологии*
Учёная степень: *доктор технических наук*
по специальности *05.13.19*
Учёное звание: *профессор*
по специальности *05.13.19 – Методы и системы защиты информации, информационная безопасность*

Основные публикации по профилю оппонируемой диссертации в научных рецензируемых изданиях за последние 5 лет (не более 15 публикаций):

1. Moldovyan N.A., Shcherbacov A.V., Eremeev M.A. Deniable-encryption protocols based on commutative ciphers // Quasigroups and related systems. 2017. Vol. 25. no. 1, pp. 95-108.
2. Михтеев М.С., Молдовян Н.А. Гибридный протокол отрицаемого шифрования, основанный на процедуре аутентификации // Вопросы защиты информации. 2017. № 1. С. 12-17.
3. Moldovyan N.A., Moldovyan A.A., Moldovyan D.N., Shcherbacov V.A. Stream Deniable-Encryption Algorithms // Computer Science Journal of Moldova. 2016. V.24. N. 1(70). P. 68-82.
4. Moldovyan N.A., Moldovyan A.A., Shcherbacov V.A. Generating Cubic Equations as a Method for Public Encryption // Buletinul Academiei de Stiinte a Republicii Moldova. Matematica. 2015. N. 3 (79). P. 60-71.
5. Молдовян Н. А., Щербаков А.В. Протокол бесключевого отрицаемого шифрования // Вопросы защиты информации. 2016. № 2. С. 9-14.
6. Moldovyan N.A., Moldovyan A.A., Berezin A.N. On Using Mersenne Primes in Designing Cryptoschemes // Int. Journal of Network Security. 2016. Vol. 18, No. 2, pp. 369-373.
7. Молдовян Н. А., Щербаков А.В. Протокол бесключевого отрицаемого шифрования // Вопросы защиты информации. 2016. № 2. С. 9-14.

8. Молдовян Н.А., Горячев А.А., Муравьев.А.В. Протокол стойкого шифрования по ключу малого размера // Вопросы защиты информации. 2015. № 1. С. 3-8.
9. Березин А.Н., Молдовян Н.А., Щербаков В.А. Общий метод построения криптосхем, основанных на трудности одновременного решения задач факторизации и дискретного логарифмирования // Вопросы защиты информации. 2014. № 2. С. 3-11.
10. Moldovyan A. A., Moldovyan N. A., Shcherbakov V. A. Bi-Deniable Public-Key Encryption Protocol Secure Against Active Coercive Adversary // Buletinul Academiei de Stiinte a Republicii Moldova. Matematica. 2014. N. 3 (76). P. 23-29.
11. Moldovyan A.A., Moldovyan N.A. Group signature protocol based on masking public keys // Quasigroups and related systems. 2014. Vol. 22. P. 133-140.
12. Moldovyan A.A., Moldovyan N.A. Practical Method for Bi-Deniable Public-Key Encryption // Quasigroups and related systems. 2014. Vol. 22. P. 277-282.
13. Морозова Е.В, Мондикова Я.А., Молдовян Н. А. Способы отрицаемого шифрования с разделяемым ключом // Информационно-управляющие системы. № 6. 2013. С. 73-78.
14. Молдовян Н. А., Рыжков А.В. Способ коммутативного шифрования на основе вероятностного кодирования. // Вопросы защиты информации. 2013. № 3. С. 3-10.

«11» октября 20 17 г. _____
(подпись)

Подпись заверяю:

...а кадров
...Д.В.Токарев