МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 2 С. 87–96

УДК 519.719.2

Synthesis of asymptotically size-optimal Boolean circuits protected from functionality inference

S. A. Lozhkin, M. S. Shupletsov, B. R. Danilov

Lomonosov Moscow State University, Moscow

Получено 11.VI.2016

Abstract. We propose several asymptotically size-optimal Boolean circuits synthesis methods that implement arbitrary Boolean functions of a given number of Boolean variables with a given protection level from functionality inference when concealing some number of local interconnections. These methods rely on the structure of Boolean circuits over arbitrary finite complete basis. Constructed by methods of generalized decomposition and universal systems of Boolean functions.

Keywords: Boolean circuits, asymptotic methods, obscuration of functionality

Синтез асимптотически оптимальных по сложности схем из функциональных элементов, защищенных от раскрытия функциональности

С. А. Ложкин, М. С. Шуплецов, Б. Р. Данилов

Московский государственный университет им. М. В. Ломоносова, Москва

Аннотация. Предлагаются методы синтеза асимптотически оптимальных по сложности схем из функциональных элементов, которые реализуют произвольные функции алгебры логики от заданного числа переменных и обладают заданным уровнем защищенности от раскрытия их функциональности при сокрытии определенного числа локальных соединений. Эти методы опираются на особенности структуры схем из функциональных элементов в произвольном базисе, построенных с использованием методов обобщенного разложения и универсальных систем функций алгебры логики.

Ключевые слова: схема из функциональных элементов, асимптотические методы, сокрытие закона функционирования

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 2, pp. 87–96 (Russian)

References

[1] Lozhkin S. A., “High-precision estimates for the complexity of control systems from some classes”, *Matem. voprosy kibernetiki*, **6** (1996), 189–214 (in Russian).

[2] Lozhkin S. A., Shiganov A. E., “High accuracy asymptotic bounds on the BDD size and weight of the hardest functions”, *Fundamenta Informaticae*, **104**:3 (2010), 239–253.

[3] Lupanov O. B., *Asymptotic estimates of complexity of control systems*, M.: Izdatel’stvo MGU, 1984 (in Russian).

[4] Lupanov O. B., “On an approach to the synthesis of control systems – principle of local coding”, *Problemy kibernetiki*, **14** (1965), 31–110 (in Russian).