Научный вестник НГТУ. – 2014. – № 1(54)

УДК 004.056; 003.26

Альтернативные формы представления булевых функций в криптографических средствах защиты информации*

С.А. КУЩ

Черкассы, Черкасский государственный технологический университет

В работе предлагается новый подход к формированию функций, используемых в криптографии и криптоанализе с использованием альтернативных форм представления булевых функций, т. е. тех которые отличаются от классической формы, которая формируется в булевом базисе И-ИЛИ-НЕТ. Как пример рассмотрен возможный порядок формирования криптографических функций с использованием альтернативной формы представления, а именно Cognate-формы представления булевых функций. Даная форма по своей сути является мультивариантной и позволяет выбирать лучший вариант из множества возможных и допустимых. Причем критерии допустимости также можно выбирать в зависимости от конкретной ситуации, так как известно, что улучшение одного критерия, как правило, ведет к ухудшению остальных. В данном случае, используя Cognate-форму, мы можем выбрать необходимое решение из множества возможных. Также показано, что использование этой формы представления булевых функций при построении криптографических функций, алгоритмов и устройств может значительно улучшить их параметры и свойства. А при использовании их в криптографических средствах защиты позволяет оптимизировать процесс логического проектирования устройств криптозащиты и улучшить показатели безопасности информационных и коммуникационных систем.

Ключевые слова: криптография, криптографические функции, криптографические свойства, алгоритмы формирования криптографических функций, Cognate-форма представления булевых функций, альтернативные формы представления булевых функций, Родственная реализация, защита информации.

ВВЕДЕНИЕ

Стремительное развитие информационных технологий оказывает существенное влияние на все стороны жизни человечества. Время массовых коммуникаций, Интернет, информатизация управления технологическими процессами в различных сферах деятельности человека привели к резкому росту потребности в обеспечении безопасности информационных систем от несанкционированного доступа и деструктивных воздействий. Как следствие, задача построения надежных телекоммуникационных систем и разработки методов оценки уровня их защищенности приобретают все большую актуальность. При этом важное место в обеспечении безопасности передачи информации играют криптографические средства защиты. В то же время опыт практического использования существующих криптографических средств защиты информации показывает, что применяемые на практике системы не всегда в состоянии обеспечить современные требования по защите информации. Поэтому задача по совершенствованию и совершенствованию средств защиты информации является важной и актуальной.

ПОСТАНОВКА ЗАДАЧИ

Целью данной работы является исследование возможностей использования альтернативных форм представления булевых функций в криптографии. Альтернативными мы называем те формы представления (ФП) булевых функций (БФ), которые отличаются от классической ФП, наиболее распространенной на сегодня, а именно алгебраической ФП, которая является

* *Статья получена 5 декабря 2013 г.*

результатом ортофункционального Ф-преобразования логической функции в эквивалентные кусочно-постоянные функции, Рида-Мюллера ФП, в которой БФ представляются в виде системы ЛФ И-СУММА ПО MOD2 - И [1], а также исследованы в последние годы ортогональная ФП [2] и Cognate-ФП [3], [4].

БФ являются одними из основных структурных элементов в большинстве современных криптографических конструкций (потоковые шифры, блочные шифры, хеш-функции и т. п.). Такие функции (системы функций), которые применяются при синтезе криптографических объектов, называют криптографическими функциями. В процессе развития средств и методов криптографического анализа выделился ряд математических требований (свойств), которым должны удовлетворять криптографические функции. Наличие подобных свойств в функциях призвано обеспечить устойчивость построенных с их помощью криптографических схем к криптографическому анализу. Примерами таких свойств являются: отсутствие корреляционных связей между значением функции и набором ее переменных фиксированной мощности [10], отсутствие в БФ низкостепенных аннигиляторов [8], отсутствие в БФ (отображении) линейных структур [9]. Множества БФ, имеющих данные свойства, выделяются в отдельные классы. К их числу относятся бент-функции, корреляционно-иммунные функции, алгебраически-иммунные функции и алгебраически-невырожденные функции. Характерной особенностью этих классов является отсутствие не только точного алгебраического описания, но также отсутствие точных выражений для оценки их мощностей. Примерами результатов исследований в этой области могут служить работы Маитра для корреляционно-иммунных функций, оценки для числа бент-функций в работах Карлето и Кротова, асимптотические оценки числа алгебраически вырожденных функций. Хотя подобные функции имеют нетривиальные линейные структуры, не обладающие необходимыми криптографическими свойствами, вместе с тем, они играют важную роль в криптоанализе.

Множество криптографических функций можно представить в форме диаграммы Венна (рис. 1).

Рис. 1. Диаграмма Венна для криптографических булевых функций

Изучение криптографических свойств происходит с использованием различных ФП БФ, таких как алгебраическая нормальная форма, числовая нормальная форма, полиномиальное представление посредством расширения поля из двух элементов, представления с помощью графов и др. При анализе криптографических свойств функций используются результаты математической кибернетики, комбинаторного анализа и алгебры. Важную роль играют и экспериментальные исследования с использованием возможностей компьютерной техники. Для того чтобы сделать вывод о возможности использования альтернативных форм представления булевых функций в криптографии и криптоанализе, необходимо провести следующие работы:

– исследование криптографических свойств и построение широких классов БФ, имеющих заданные свойства, а также построение функций, имеющих экстремальные параметры в различных ФП;

– исследование криптографических свойств БФ, реализованных в различных, в том числе, альтернативных ФП в конкретных криптографических системах;

– построение множеств БФ, имеющих два или более необходимых криптографических свойства, а также другие, которые могут появиться при проведении исследований.

Рис. 2. Последовательность формирования криптографической функции в Cognate-форме представления

Хотя изучение свойств функций конкретных криптографических систем стало типичной задачей любого криптографического анализа, в то же время существует ряд задач, решение которых позволит подняться на новый уровень формирования криптографических систем. К ним относятся, например:

– вычисление мощностей (или их оценок) некоторых классов БФ, например, БФ, обладающих свойством корреляционной иммунности заданного порядка, бент-функции, k-бент-функции [7] в различных ФП и т. п.;

– описание групп инвариантности конкретных криптографических свойств;

– разработка алгоритмов аппроксимации произвольной функции функциями из заданного класса.

Учитывая это, набор существующих криптографических свойств БФ и их отражений в различных ФП ни в коем случае нельзя считать завершенным. Практика показывает, что методы

построения криптографических функций и криптографического анализа в наше время продолжают развиваться и результаты такого развития выдвигают к криптографическим функциям все новые и новые требования. Именно поэтому поиск новых вариантов формирования криптографических функций является важной научной и практической задачей сегодняшнего дня. В работах [1–5] показано и доказано, что использование альтернативных ФП позволяет упростить формирование и техническую реализацию БФ, что может найти применение при формировании криптографических функций, а также в технических средствах защиты информации.

В качестве примера рассмотрим возможный порядок формирования криптографических функций, используя альтернативные ФП. Пользуясь разработанным ранее автором алгоритмом формирования БФ в Cognate-ФП [5] (известна также под названием Родственная ФП [3, 4]) и методом, описанным в [6], можно предложить описанную ниже последовательность формирования криптографической функции частности в Cognate-ФП (рис. 2).

Рассмотрим более детально каждый пункт этой последовательности.

1. **Формирование начального ансамбля близких функций.** Начальный ансамбль $f_{\text{б}}$ близких к номинальным БФ f_n формируется как множество БФ, имеющих одиночные Cognate-близости C_{gn} к номинальным БФ – $C_{gn} = \frac{1}{2^n}$. Это дает ансамбль, состоящий формально из 2^{n+1} БФ, но все они обязательно подлежат проверке на приемлемость в комплекте с номинальными БФ.

2. **Формирование системы ограничений по нелинейности и автокорреляции криптографических БФ**. Используется в качестве исходной информации, задающей основные параметры вычислительного метода формирования криптографических БФ с помощью градиентного поиска.

3. **Процедуры вычислительного поиска криптографической БФ методом градиентного спуска.** По введенным ограничениям с использованием метода градиентного спуска осуществляется вероятностный поиск БФ. Результатом является случайно сформированная БФ, удовлетворяющая необходимым значением нелинейности и автокорреляции.

4. **Система ограничений на компонентные криптографические БФ и их линейные комбинации.** Используется в качестве исходной информации, задающей основные параметры отбора случайно сложившихся БФ, которые удовлетворяют требуемым значениям нелинейности и автокорреляции.

5. **Процедуры проверки выполнения системы ограничений на компонентные функции и их линейные комбинации.** Сформированные БФ с требуемыми значениями нелинейности и автокорреляции подвергаются проверке на соответствие системным требованиям, т. е. на пригодность использования в совокупности с другими БФ.

6. **Проверка элементов первоначального ансамбля близости.** Формирование рабочего ансамбля приемлемо-близких БФ осуществляется вычеркиванием тех элементов ансамбля, которые не обеспечивают фактическую близость.

7. **Формирование множества компонентных криптографических БФ и соответствующей таблицы замен.**

8. **Попарное сравнение по стандартной шкале метода анализа иерархий (МАИ) критериев качества и альтернатив.**

9. **Избрание оптимального варианта для реализации.** На базе отобранной БФ синтезируется устройство, реализующее заложенную в него логику преобразований.

Таким образом, Cognate-реализация БФ отличается от классической выполнением дополнительный этапов:

– формированием первоначального ансамбля приемлемых вариантов;

– рабочего ансамбля вариантов после проверки и урезание элементов первоначального ансамбля;

– множества критериев оценки качества вариантов реализации;

– множества «близких» альтернатив;

– попарным сравнением по стандартной шкале МАИ критериев качества и альтернатив;

– избранием оптимального варианта для реализации.

Использование Cognate-реализации дает основу для существенного уменьшения аппаратурных затрат при реализации БФ в криптографических устройствах.

ЗАКЛЮЧЕНИЕ

Предложенный в статье анализ на примере Cognate-ФП БФ показывает, что использование альтернативных ФП БФ при построении криптографических функций, алгоритмов и устройств может значительно улучшить их параметры и свойства, а при использовании их в криптографических средствах защиты позволяет оптимизировать процесс логического проектирования устройств криптозащиты и улучшить показатели безопасности информационных и коммуникационных систем. Поэтому это направление остается актуальным с научной и практической точки зрения для ученых и разработчиков систем защиты информации.

СПИСОК ЛИТЕРАТУРЫ

[1] Каталог-справочник «Классические и альтернативные минимальные формы логических функций»: монография / Ю.А. Кочкарев, Н.Л. Казаринова, Н.Н. Пантелеева, С.А. Шакун**;** под ред. Ю.А. Кочкарева. – Черкассы: ИПМЭ, 1999. – 195 с.

[2] **Kochkarev Y.A.** Ortogonal forms of presentation of boolean functions in device blocks / Y.A. Kochkarev, I.I. Osipenkova, E.N. Panasko // Вестник Черкасского государственного технологического университета. – 2009. – Спецвыпуск. – С. 39–42.

[3] **Кочкарев Ю.А.** Представление и реализация логических функций в родственной форме / Ю.А. Кочкарев, С.А. Кущ // Электронное моделирование. – 2011. – № 6. – С. 73–80.

[4] **Кочкарев Ю.А.** Родственная реализация логических функций на основе их представления в изоморфной форме / Ю.А. Кочкарев, С.А. Кущ // Электронное моделирование. – 2012. – № 4. – С. 119–123.

[5] **Кочкарев Ю.А.** Технология Cognate-реализации логических функций / Ю.А. Кочкарев, С.А. Кущ // Вестник Черкасского государственного технологического университета. – 2013. – № 3. – С. 35–38.

[6] Вероятностная модель формирования нелинейных узлов замен для симметричных криптографических средств защиты информации / Л.С. Сорока, А.А. Кузнецов, И.В. Московченко, С.А. Исаев // Системы обработки информации. – 2009. – Вып. 3 (77). – С. 101–104.

[7] **Токарева Н.Н**. Бент-функции с более сильными свойствами нелинейности: k-бент-функции / Н.Н. Токарева // Дискретный анализ и исследование операций. Сер. 1. – 2007. – Т. 14. – № 4. – С. 76–102. DOI: 10.1134/S1990478908040133

[8] **Courtois N.** Algebraic attacks on stream ciphers with linear feedback / N. Courtois, W. Meier // Lecture Notes in Computer Science. – 2003. – Vol. 2656. – P. 345–359. DOI: 10.1007/3-540-39200-9_21

[9] **Evertse J.H.** Linear Structures in Block Ciphers / J.H. Evertse // Proceedings of Eurocrypt'87. – 1987. – P. 249–266.

[10] **Siegenthaler T.** Correlation-immunity of nonlinear combining functions for cryptographic applications / T. Siegenthaler // IEEE Trans. on Inform. Theory. – 1984. – Vol. 5. – Pp. 776–780.

REFERENCES

[1] Kochkarev Yu., Kazarinova N., Panteleeva N., Shakun S. Katalog-spravochnik «Klassicheskie i al'ternativnye minimal'nye formy logicheskikh funktsii». Monografiia [Catalog-Directory «Classic and alternative minimum form of logical functions.» Monograph], Cherkasy, 1999, 195 p.

[2] Kochkarev Yu., Osipenkova I., Panasko E. Ortogonal forms of presentation of boolean functions in device blocks. *Vestnik Cherkasskogo gosudarstvennogo tekhnologicheskogo universiteta – Bulletin of Cherkasy state technological university*, 2009, pp. 39–42.

[3] Kochkarev Yu., Kushch S., Predstavlenie i realizatsiia logicheskikh funktsii v rodstvennoi forme [Justification of a Cognate-form of representation and realization of logical functions]. 2010. Elektronnoe modelirovanie – *Electronic Modeling*, v. 33(6), pp. 73–80.

[4] Kochkarev Yu., Kushch S. Rodstvennaia realizatsiia logicheskikh funktsii na osnove ikh predstavleniia v izomorfnoi forme [A Cognate-realization of logic functions on the basis of their representation in isomorphic form], 2012, *Elektronnoe modelirovanie – Electronic Modeling*, v. 34(4), pp. 119–123.

[5] Kochkarev Yu., Kushch S., Tekhnologiia Cognate-realizatsii logicheskikh funktsii [Technology of Cognate-implementation of logic functions], 2011, *Vestnik Cherkasskogo gosudarstvennogo tekhnologicheskogo universiteta – Bulletin of Cherkasy state technological university*, 3, pp. 35–38.

[6] Veroiatnostnaia model' formirovaniia nelineinykh uzlov zamen dlia simmetrichnykh kriptograficheskikh sredstv zashchity informatsii [Probabilistic model of substitution box generation for symmetric cryptographic methods of information

security], L.S. Soroka, A.A. Kuznetsov, I.V. Moskovchenko, S.A. Isaev. *Sistemy obrabotki informatsii – Information processing system*, CUPS, 2009, v. 3 (77), pp. 101–104.

[7] Tokareva N.N. Bent functions with stronger nonlinear properties: K-bent functions. *Journal of Applied and Industrial Mathematics*, vol. 2, issue 4, pp. 566–584. DOI: 10.1134/S1990478908040133.

[8] Courtois N., Meier W. Algebraic attacks on stream ciphers with linear feedback. *Lecture Notes in Computer Science*, 2003, vol. 2656, pp. 345–359. DOI: 10.1007/3-540-39200-9_21.

[9] Evertse J.H. Linear Structures in Block Ciphers. *Proceedings of Eurocrypt'87*, 1987, pp. 249–266.

[10] Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. on Inform. Theory*, 1984, vol. 5, pp. 776–780.

Кущ Сергей Александрович, кандидат технических наук, действительный член Institute of Electrical and Electronics Engineers (IEEEE), старший преподаватель кафедры информатики и информационной безопасности Черкасского государственного технологического университета, Украина. Основное направление научных исследований – использование различных форм представлений булевых функций в логическом проектировании и защите информации. Имеет 15 публикаций. E-mail: kushch@eee.org

S.A. Kushch

Alternative forms of representation of Boolean functions in Cryptographic Information Security Facilities

The work suggests a new approach to the formation of the functions used in cryptography and cryptanalysis with use of alternative forms of Boolean functions representation. Alternative forms of Boolean functions representation is forms which differ from the classical form, which formed in the boolean basis AND-OR-NOT. As an example, is consider the procedure of formation of cryptographic functions with the use of alternative forms of representation, namely Cognate-forms of Boolean functions representations. This form inherently is multivariate and allows you to choose the best option from a set of possible and permissible. Moreover admissibility criteria can also be selected depending on the particular situation, since it is known that an improvement in one criterion usually leads to a deterioration of the others. In this case, using Cognate-form, we can select the necessary solution of many possible. It is shown that the use of this forms of representation of Boolean functions in the construction of cryptographic functions, algorithms and devices can be significantly improve their parameters and properties. And when they are used in cryptographic means of protection to optimize the process of logical design of cryptographic devices and improve the security of information and communication systems.

Key words: cryptography, cryptographic functions, cryptographic properties, forming algorithms cryptographic functions, Cognate-forms of Boolean functions representations, alternative forms of representation of Boolean functions, Cognate implementation, information security.