Д. В. Закаблуков

СИНТЕЗ СХЕМ ИЗ ОБРАТИМЫХ ЭЛЕМЕНТОВ

Потери энергии являются важным фактором, который необходимо учитывать при разработке цифровых схем. Часть проблемы рассеяния энергии связана с использованием неидеальных технологических элементов, другая часть — с принципом Ландауэра [1], который гласит, что в любой вычислительной системе, независимо от ее физической реализации, при потере 1 бита информации выделяется количество энергии не менее чем $k \cdot T \cdot \ln 2$ Дж, где k — постоянная Больцмана, а T — абсолютная температура вычислительной системы. Можно рассчитать, что количество энергии, которое должно выделиться из-за потери информации в современном процессоре, составляет $1{,}4 \cdot 10^{18} \cdot k \cdot T \cdot \ln 2$ Дж/с. При температуре процессора 80єС (пиковая нагрузка) количество выделяемой энергии составит примерно 4,7 мВт. В действительности же современные процессоры выделяют в 500 раз больше энергии из-за потери информации [2], т. е. примерно 2,35 Вт. Если в будущем удастся достигнуть плотности размещения логических устройств в 10^{17} на кубический сантиметр [3], то при комнатной температуре во время работы на частоте в 10 ГГц такое количество стандартных устройств должно выделять более $3 \cdot 10^6$ Вт энергии.

Обратимые вычисления не приводят к потере информации во время вычислительного процесса, а значит, и к рассеянию энергии. Беннет показал [4], что нулевой уровень рассеяния энергии возможен только в случае, когда все элементы схемы являются обратимыми. Как результат, обратимость в ближайшем будущем, по-видимому, станет главным требованием к синтезу схем. Обратимая логика может быть применена в различных технологиях, таких как синтез CMOS-микросхем с ультранизким потреблением энергии, оптические вычисления, квантовые вычисления, термодинамические технологии, технологии ДНК и нанотехнологии.

Большинство элементов, используемых в настоящее время в синтезе стандартных цифровых микросхем, не являются обратимыми (кроме элемента NOT). В то же время к обратимым элементам относятся контролируемая инверсия (CNOT), предложенная Фейнманом, элемент Тоффоли (CCNOT), элемент Фредкина и ряд других. Все эти элементы были достаточно хорошо изучены, однако не было предложено эффективного алгоритма синтеза схем минимальной сложности из обратимых элементов.

Традиционные методы синтеза используют, помимо прочих критериев, количество элементов в схеме в качестве меры ее сложности. В отношении обратимой логики мы имеем еще один фактор, который более важен, чем количество элементов в схеме, — количество выходов с «мусором». Это такие выходы, которые несут информацию, не являющуюся необходимой для дальнейших вычислений. Количество выходов с «мусором» важно, потому что именно они приводят к потере информации и, как следствие, к потреблению дополнительной энергии и выделению тепла во время вычислений.

В работе [5] было доказано, что схема, состоящая из обратимых элементов NOT, CNOT и CCNOT, реализует четную подстановку, если количество входов схемы больше трех. При этом для любой четной подстановки из S_N, $N = 2^n$, $n \geq 4$, существует реализующая ее схема из обратимых логических элементов без дополнительной памяти. Если же подстановка нечетная, то для ее реализации потребуется максимум один дополнительный вход [5].

В работе [6] был представлен алгоритм синтеза схем из обратимых логических элементов, основанный на теории групп. Временная сложность реализации схемы с n входами для данного алгоритма равна $10/3 \cdot n^2 \cdot 2^n$. Реализуемое преобразование рассматривается как подстановка на множестве двоичных наборов. Она представляется в виде произведения циклов длины 3 специ-

ального вида. Затем каждый из этих циклов реализуется стандартным образом. Основным недостатком данного алгоритма является большое количество элементов в итоговой схеме.

В настоящее время разрабатывается новый алгоритм синтеза схем из обратимых двоичных элементов, основанный на теории групп. Его отличие от предыдущего заключается в том, что подстановка представляется в виде произведения транспозиций, а не циклов длины 3. Алгоритм основан на доказательстве генерации знакопеременной группы подстановками, соответствующими обратимым элементам, приведенным в работе [5].

Для подстановки (10, 30, 14, 22, 18) исходный алгоритм дает схему, состоящую из 56 обратимых элементов [6]. Новый же алгоритм дает схему, состоящую из 36 обратимых элементов. Направлением дальнейших исследований является оптимизация существующего алгоритма для уменьшения количества элементов в схеме. Для рассмотренного примера простейшие оптимизации позволяют сократить количество элементов до 34.

Предлагаемый алгоритм синтеза предполагается использовать впоследствии для исследования зависимости сложности схемы от цикловой формы реализуемой ею подстановки, которая зависит в том числе и от количества дополнительной памяти.

СПИСОК ЛИТЕРАТУРЫ:

1. *Landauer R.* Minimal energy dissipation in logic // Landauer R., Keyes R.W. IBM J. Research and Development, March 1970. P. 152–157.
2. *Nielsen M., Chuang I.* Quantum computation and quantum information. Cambridge University Press, 2000.
3. *Merkle R. C.* Helical logic // Merkle R.C., Drexler K.E. Nanotechnology. 1996. № 7. P. 325–339.
4. *Bennett C. H.* Logical reversibility of computation // IBM Journal of Research and Development. November 1973. № 17. P. 525–532.
5. *Закаблуков Д. В.* Исследование схем из обратимых логических элементов // Закаблуков Д. В., Жуков А. Е. Информатика и системы управления в XXI веке: Сборник трудов № 9 молодых ученых, аспирантов и студентов. М.: МГТУ им. Н. Э. Баумана, 2012. С. 148–157.
6. *Yang G., Song X., Hung W., Xie F., Perkowski M.* Group Theory Based Synthesis of Binary Reversible Circuits // The 3rd Annual Conference on Theory and Applications of Models of Computation, 2006. P. 365–374.

В. Г. Иваненко, Я. И. Пивошенко

СПОСОБ ЗАЩИТЫ АВТОРСКОГО ПРАВА НА АУДИОСИГНАЛЫ, ОСНОВАННЫЙ НА ПАКЕТНОЙ ВЕЙВЛЕТ-ДЕКОМПОЗИЦИИ И ЧАСТОТНОМ МАСКИРОВАНИИ

Проблема защиты авторского права на представленную в электронном виде информацию включает в себя помимо проблемы права собственности и доказательства этого права проблему защиты от несанкционированного копирования. Среди технических средств защиты авторских прав на аудиоданные наиболее перспективными являются технологии применения цифровых водяных знаков (ЦВЗ) [1].

ЦВЗ — это малообъемная дополнительная информация, внедряемая в запись и содержащая идентифицирующую информацию о законном владельце для осуществления последующей возможности подтверждения авторского права. Международная федерация звукозаписывающей