Украинский математический конгресс – 2009

В.Е.Федюкович (Интропро, Киев, Украина)

О методе принятия решений парой конечных автоматов

Рассматриваются интерактивные системы (interactive proof system) [1, 2] для задач распознавания языка. Рассматриваются языки класса сложности NP, допускающие принятие решения за время, растущее асимтотически полиноминально с размером задачи при использовании NP-свидетельства (witness). Такие системы является парой конечных автоматов, которые выполняют вычисления и обмениваются сообщениями, так, что автомат проверяющего принимает решение о принадлежности входного слова языку, а автомат доказывающего знает свидетельство. Требуется, чтобы автомат проверяющего всегда принимал решение за полиномиальное время, в том числе для NP-полных задач. Изучаются интерактивные системы, в которых автомат проверяющего принимает неверные решения с низкой вероятностью, а также не получает какой-либо информации о свидетельстве (свойства witness hiding и zero knowledge). Изучаются системы, построенные на основе свойства гомоморфизма используемой схемы привязки (commitment scheme).

Ранее были получены интерактивные системы (протоколы) для задач проверки утверждений о пороге для ошибки в искаженном кодовом слове кода Гоппы [3], пороге для количества элементов в разности множеств [4], существовании определенного количества копий строки-шаблона в строке-тексте [5, 6], существовании цикла Гамильтона в ориентированном графе [7, 8, 9]. Были также предложены новая схема привязки к элементу конечного поля [10], полиномиальное представление строк [5, 6] и графов [7, 8, 9], схема электронной подписи на основе протокола для проверки утверждения о множествах [4]. Основным результатом этой работы является

Теорема 1 *Для любого языка* $\mathbb{L}$*, заданного уравнением над конечным полем, для NP-свидетельства* w*, допускающего проверку* $x \in \mathbb{L}$

$$\mathbb{L} = \{x \mid f_L(z) \equiv 0, \quad f_L(z) = F_L(z, x, w)\}$$

и для любой схемы привязки, имеющей свойство аддитивного гомоморфизма, существует интерактивная система для распознавания языка $\mathbb{L}$*, такая, что имеются свойства полноты, корректности, знания, специального нулевого разглашения в модели с честным проверяющим.*

Значения линейных полиномов использовались как ответы доказывающего в интерактивной системе Чома-Эвертсе-ВанДеГраафа [11]. Запросы проверяющего, выбранные из множества с большим количеством элементов, использовались в интерактивной системе Шнорра [12]. Особенностью предложенного протокола является использование проверяющим полиномов, полученных из $F_L()$ путем замены NP-свидетельства на ответы доказывающего. Верхняя оценка вероятности ошибки при

принятии решения $O\left(\frac{\deg(f_L(z))}{q}\right)$ получена исходя из максимального количества корней полинома, что убывает экспоненциально быстро с ростом $|q|$. Протокол является аргументом при использования схемы привязки, имеющей вычислительно-стойкое свойства связывания; если свойство связывания является безусловным, то протокол является доказательством. Протокол имеет моделирующий алгоритм, такой, что моделируемая стенограмма неотличима от всех стенограмм протоколов с доказывающим, в которых запросы проверяющего совпадают.

[1] *Goldwasser S., Micali S., Rackoff C.* The knowledge complexity of interactive proof systems // *SIAM J. Comput.* — 1989. — Vol. 18, no. 1. — Pp. 186–208.

[2] *Н.П. Варновский.* Типы нулевого разглашения. — Рукопись. — 2002.

[3] *Fedyukovych V.* Argument of knowledge of a bounded error. — Cryptology ePrint Archive, Report 2008/359. — 2008.

[4] *В.Е. Федюкович.* Изменчивые ключи подписи // Безопасность информации в информационно-телекоммуникационных системах. — 2007.

[5] *Fedyukovych V., Sharapov V.* A protocol for K-multiple substring matching. — Cryptology ePrint Archive, Report 2008/357. — 2008.

[6] *В.Е. Федюкович, В.Г. Шарапов.* Протокол демонстрации K-кратного вхождения строки // Информационные технологии и системы (ИТиС'08). — 2008. — Pp. 459–466.

[7] *Fedyukovych V.* An argument for Hamiltonicity. — Cryptology ePrint Archive, Report 2008/363. — 2008.

[8] *В.Е. Федюкович.* Протокол аргумента для цикла Гамильтона // Математика и безопасность информации. — 2008.

[9] *Fedyukovych V.*. Protocols for graph isomorphism and hamiltonicity // Central European Conference on Cryptography. — 2009.

[10] *В.Е. Федюкович.* Об алгебраических операциях над шифротекстом // Безопасность информации в информационно-телекоммуникационных системах. — 2009.

[11] *Chaum D., Evertse J.-H., van de Graaf J.* An improved protocol for demonstrating possession of discrete logarithms and some generalizations. // EUROCRYPT. — 1987. — Pp. 127–141.

[12] *Schnorr C.-P.* Efficient signature generation by smart cards. // *J. Cryptology.* — 1991. — Vol. 4, no. 3. — Pp. 161–174.