Модель невлияния для квантовых автоматов

И. Ю. Терёхина

В работе строится обобщение автоматной модели невлияния на случай квантовых автоматов. Доказывается «теорема раскрутки», описывающая достаточные условия безопасности.

Ключевые слова: конечные автоматы, безопасность системы, модель невлияния.

1. Введение

Формальное доказательство безопасности компьютерных систем является необходимым условием соответствия высоким классам защищенности в различных нормативных документах, начиная с так называемой «Оранжевой книги» (Trusted Computer System Evaluation Criteria, [1]). Классическим примером формальной модели безопасности компьютерных систем является модель невлияния.

Основная идея понятия невлияния была предложена Гогеном и Месгауэром в 1982 году [2]: «Группа лиц, использующая определенное множество команд, не оказывает влияния на другую группу лиц, если те действия, которые проводит первая группа со своими командами, не оказывают эффекта на то, что может увидеть вторая группа». Компьютерная система моделируется конечным детерминированным автоматом, а условие невлияния формулируется в терминах глобальных условий на поведение автомата.

В 1992 году Московитц и Костич в работе [3] рассмотрели модель невлияния применительно к системе из двух пользователей с различными уровнями доступа. В результате естественных предположений о структуре входного алфавита и множества состояний удалось сформулировать «теорему раскрутки» — утверждение о локальных

необходимых и достаточных условиях безопасности — в терминах переходов автомата на множестве однобуквенных слов. Другими словами, безопасность системы была явно сведена к анализу функции переходов. В работе [3] было также приведено обобщение модели на случай недетерминированных автоматов. Дальнейшее обобщение на случай вероятностных автоматов было сделано в 1999 году А. В. Галатенко [4].

В последние годы резко вырос интерес к квантовым моделям вычислений. Поэтому становится необходимым перевести модели классических вычислений на язык квантовых. В 1997 году было введено понятие квантового автомата для квантовых систем [5]. В 2013 году было предложено обобщение классической модели невлияния на случай квантовых систем [6].

В данной работе представлено обобщение модели невлияния Московитца-Костича на случай квантовых автоматов.

Автор выражает глубокую благодарность своему научному руководителю, к.ф.-м.н., с.н.с. А. В. Галатенко за постановки задач и внимание к работе.

2. Основные понятия и результаты

Пусть Σ — некоторое конечное непустое множество (алфавит). Обозначим через Σ^* всевозможные конечные последовательности (слова) элементов из Σ, ε — пустое слово из Σ^*.

Пусть $n \in \mathbb{N}$.

Определение 1. Конечный квантовый автомат — четверка $\langle S, \Sigma, \delta, M \rangle$, где:

1) S — n-мерное гильбертово пространство над полем комплексных чисел. Содержательно множество S задает состояния системы;
2) Σ — конечное непустое множество (задающее входной алфавит);
3) $\delta : S \times \Sigma \to S$ — функция переходов, удовлетворяющая условию $\forall a \in \Sigma$, $\forall s \in S$: $\delta(s, a) = U_a s$, где U_a — унитарный оператор, соответствующий входному символу a;
4) M — множество линейных операторов в пространстве S, доступные измерения состояния системы.

Функцию переходов можно продолжить по мультипликативности: $\delta : S \times \Sigma^* \to S$, $\delta(s, \varepsilon) = s$.

Содержательно опишем функционирование квантового автомата. Пусть автомат в некоторый момент времени находился в состоянии $s \in S$ и получил на вход слово $\alpha = a_1 \dots a_n \in \Sigma^*$. Автомат под действием α переходит в новое состояние $s' = \delta(s, \alpha) = U_{a_n} \dots U_{a_1} s$, где U_{a_i} — унитарный оператор, соответствующий входному символу a_i. Узнать, в каком состоянии находится автомат в данный момент, можно при помощи измерений из множества M, при этом автомат перейдет в новое состояние $s'' = Es'$, где $E \in M$.

Аналогично [3], [4] будем рассматривать многоуровневую систему, состоящую из 2 уровней или типов пользователей: пользователь верхнего уровня H и пользователь нижнего уровня L. Пусть множества входных символов, соответствующих H и L, не пересекаются. Пользователь H может наблюдать все пространство S, пользователь L — только некоторое подпространство S_L. В соответствии с идеологией невлияния требуется, чтобы любые действия H не изменяли компонент вектора состояний L, а L не смог бы узнать (измерить) какие-либо компоненты вне доступного подпространства. Формализуем эти предположения:

- Пусть $\{|\psi_i\rangle\}_{i=0}^{n-1}$ — ортонормированный базис S. Пространство S представлено в виде прямого произведения $S = S_L \times S_H$, размерность S_L равна l, и $\{|\psi_i\rangle\}_{i=0}^{l-1}$ — базис S_L, $\{|\psi_i\rangle\}_{i=l}^{n-1}$ — базис S_H.
- Входной алфавит Σ удовлетворяет условию $\Sigma = \Sigma_L \cup \Sigma_H$, где Σ_L — входы, соответствующие пользователю L, Σ_H — входы, соответствующие пользователю H, причем $\Sigma_L \cap \Sigma_H = \varnothing$.
- Множество возможных измерений состояния для пользователей H и L разделено: $M = M_L \cup M_H$, причем $M_L \cap M_H = \varnothing$.

Любое состояние $s \in S$ можно представить, в следующем виде:

$$s = \sum_{i=0}^{n-1} c_i |\psi_i\rangle.$$

Пусть $k \leqslant n$ — количество компонент вектора состояний, которые могут быть измерены посредством оператора измерения $E \in M$.

Тогда E можно представить в следующем виде:

$$E = \sum_{i,j=0}^{k-1} e_{ij}|\psi_i\rangle\langle\psi_j|.$$

Измерение $E \in M$, $E = \sum_{i,j=0}^{l-1} e_{ij}|\psi_i\rangle\langle\psi_j|$, действует на состояние $s \in S$, $s = \sum_{k=0}^{n-1} c_k|\psi_k\rangle$, следующим образом [6]:

$$Es = \sum_{i,j=0}^{k-1} e_{ij}|\psi_i\rangle\langle\psi_j| \sum_{t=0}^{n-1} c_k|\psi_t\rangle = \sum_{i,j=0}^{k-1} e_{ij}c_j|\psi_i\rangle.$$

Определение 2. Расстоянием между результатами измерения $E \in M$ состояний $s_1, s_2 \in S$, будем называть:

$$d_E(s_1, s_2) = ||Es_1 - Es_2||,$$

где $||s|| = \sqrt{< s|s >}$ — норма в S.

Определение 3. Назовем сжатием входа функцию $F : \Sigma^* \to \Sigma_L^*$, определенную следующим образом. Пусть $\alpha = a_1a_2 \dots a_n \in \Sigma^*$. Тогда

$$F(\alpha) = a'_1a'_2 \dots a'_n,$$

где

$$a'_i = \begin{cases} a_i, & \text{если } a_i \in \Sigma_L; \\ \varepsilon, & \text{если } a_i \in \Sigma_H \cup \{\varepsilon\}. \end{cases}$$

Пусть $\pi_L : S \to S_L$ — ортогональная проекция вектора состояний пространства S на подпространство S_L. Аналогично, $\pi_H : S \to S_H$ — ортогональная проекция на подпространство S_H.

Пусть дан квантовый автомат $\mathcal{W} = \langle S = S_H \times S_L, \Sigma = \Sigma_H \sqcup \Sigma_L, \delta, M = M_H \sqcup M_L \rangle$.

Определение 4. $\mathcal{W}$ является безопасным квантовым автоматом, если $\forall \alpha \in \Sigma^*$, $\forall E \in M_L$, $\forall s \in S$ выполнено следующее условие:

$$d_E(\delta(s, \alpha), \delta(s, F(\alpha))) = 0,$$

Содержательно условие безопасности означает, что с точки зрения пользователя L система выглядит одинаково, какие бы действия

ни предпринимал пользователь H. Другими словами, H не может повлиять на L. Сформулируем условия на матрицы переходов, гарантирующие безопасность системы.

Обозначим через O матрицу, состоящую из одних нулей, через I — единичную матрицу.

Определение 5. Оператор U будем называть L-диагональным, если его матрица размерности $n \times n$ имеет вид:

$$U = \begin{pmatrix} I & O \\ O & U' \end{pmatrix},$$

где I — единичная матрица размерности $l \times l$, а U' — некоторая унитарная матрица размерности $(n-l) \times (n-l)$.

Определение 6. Оператор U будем называть L-стационарным, если его матрица размерности $n \times n$ имеет вид:

$$U = \begin{pmatrix} U' & O \\ O & U'' \end{pmatrix},$$

где U' — унитарная матрица размерности $l \times l$, а U'' — унитарная матрица размерности $(n-l) \times (n-l)$.

Легко увидеть, что L-диагональные и L-стационарные операторы унитарны.

Определение 7. Будем говорить, что для пользователя L выполняется условие локализации измерений, если L с помощью измерений M_L может измерить только ту часть вектора состояний, которая принадлежит S_L.

Сформулируем достаточные условия безопасности.

Теорема 1. *Пусть $\forall a \in \Sigma_H$ оператор U_a L-диагонален, и $\forall a \in \Sigma_L$ оператор U_a L-стационарен. Тогда для произвольных $\alpha \in \Sigma^*$ и $s \in S$ выполнено следующее равенство:*

$$\pi_L(\delta(s, \alpha)) = \pi_L(\delta(s, F(\alpha))).$$

Следствие 1. *Пусть $\forall a \in \Sigma_H$ оператор U_a L-диагонален, и $\forall a \in \Sigma_L$ оператор U_a L-стационарен. Пусть для пользователя L выполняется условие локализации измерений. Тогда квантовый автомат W безопасный.*

Замечание. Для выполнения условия локализации измерений достаточно, чтобы для любого оператора измерений $E \in M_L$ подпространство S_H входило в ядро. В терминах матриц это условие означает, что правый блок размера n на $n - l$ является нулевым.

3. Вспомогательные утверждения

Лемма 1. *Пусть $s \in S$, U — произвольный L-диагональный оператор. Тогда $\pi_L(s) = \pi_L(Us)$.*

Доказательство. Состояние s запишем в следующем виде:

$$s = \begin{pmatrix} s_L \\ s_H \end{pmatrix}.$$

Здесь s_L — вектор, содержащий l компонент.

Тогда, в силу L-диагональности U, справедливы следующие равенства:

$$Us = \begin{pmatrix} I & O \\ O & U' \end{pmatrix} \begin{pmatrix} s_L \\ s_H \end{pmatrix} = \begin{pmatrix} s_L \\ U's_H \end{pmatrix},$$
$$\pi_L(s) = \pi_L(Us) = s_L.$$

Лемма 2. *Пусть $s_1, s_2 \in S$ такие, что $\pi_L(s_1) = \pi_L(s_2)$, U — некоторый L-стационарный оператор. Тогда $\pi_L(Us_1) = \pi_L(Us_2)$.*

Доказательство. Запишем s_1, s_2 в виде

$$s_i = \begin{pmatrix} s_{iL} \\ s_{iH} \end{pmatrix},$$

где s_{iL} — вектор, содержащий l компонент, $i = 1, 2$.

Тогда из L-стационарности оператора U вытекают следующие равенства:

$$Us_1 = \begin{pmatrix} U' & O \\ O & U'' \end{pmatrix} \begin{pmatrix} s_{1L} \\ s_{1H} \end{pmatrix} = \begin{pmatrix} U's_{1L} \\ U''s_{1H} \end{pmatrix}$$
$$Us_2 = \begin{pmatrix} U' & O \\ O & U'' \end{pmatrix} \begin{pmatrix} s_{2L} \\ s_{2H} \end{pmatrix} = \begin{pmatrix} U's_{2L} \\ U''s_{2H} \end{pmatrix}$$

Так как $\pi_L(s_1) = \pi_L(s_2)$, $s_{1L} = s_{2L}$. Следовательно, $U's_{1L} = U's_{2L}$ и $\pi_L(Us_1) = \pi_L(Us_2)$.

4. Доказательство теоремы 1

Запишем состояние s в следующем виде:

$$s = \begin{pmatrix} s_L \\ s_H \end{pmatrix},$$

где s_L — вектор, содержащий l компонент.

Проведем доказательство индукцией по длине входного слова $\alpha \in \Sigma^*$. При $|\alpha| = 0$, то есть $\alpha = \varepsilon$, равенство $\pi_L(\delta(s, \alpha)) = \pi_L(\delta(s, F(\alpha)) = s$ очевидно.

Предположим, что условие теоремы верно для всех слов длины n. Рассмотрим произвольное слово α длины $n+1$, $\alpha = \alpha' a_{n+1}$. Обозначим $\delta(s, \alpha') = s'$, $\delta(s, F(\alpha')) = s''$

Рассмотрим 2 возможных случая:

- $a_{n+1} \in \Sigma_L$. Тогда

  $$\delta(s, \alpha) = U_{a_{n+1}} s', \delta(s, F(\alpha)) = U_{a_{n+1}} s'',$$

  причем оператор $U_{a_{n+1}}$ L-стационарен. По предположению индукции $\pi_L(s') = \pi_L(s'')$. По определению $F(a_{n+1}) = a_{n+1}$. По лемме 2 $\pi_L(\delta(s', a_{n+1})) = \pi_L(\delta(s'', F(a_{n+1})))$. Следовательно, $\pi_L(\delta(s, \alpha)) = \pi_L(\delta(s, F(\alpha)))$.
- $a_{n+1} \in \Sigma_H$. Тогда

  $$\delta(s, \alpha) = U_{a_{n+1}} s', \delta(s, F(\alpha)) = s'',$$

  причем оператор $U_{a_{n+1}}$ L-диагонален. По предположению индукции $\pi_L(s') = \pi_L(s'')$. По определению $F(a_{n+1}) = \varepsilon$. По лемме 1 $\pi_L(\delta(s', a_{n+1})) = \pi_L(\delta(s'', F(a_{n+1})))$. Следовательно, $\pi_L(\delta(s, \alpha)) = \pi_L(\delta(s, F(\alpha)))$.

5. Заключение

В работе предложено обобщение модели невлияния Московитца-Костича на случай квантовых автоматов. Получены достаточные условия для обеспечения безопасности, показывающие, что для обеспечения безопасности квантового автомата достаточно ограничить операторы переходов и измерений.

Список литературы

[1] Trusted Computer System Evaluation Criteria. DoD 5200.28-STD, December 26, 1985.

[2] Goguen J. A., Meseguer J. Security policies and security models // Proceedings of the 1982 IEEE Symposium on Security and Privacy. — P. 11–20.

[3] Moskowitz I. S., Costich O. L. A classical automata approach to noninterference type problems // Proc. Comp. Security Found. Workshop 5. — IEEE Press, Franconi, 1992. — P. 2–8.

[4] Галатенко А. В. Об автоматной модели защищенных компьютерных систем // Интеллектуальные системы. — 1999. — Т. 4, вып. 3–4. — С. 263–270.

[5] Moore C., Crutchfield J. P. Quantum Automata and Quantum Grammars. [http://arxiv.org/pdf/quant-ph/9707031.pdf]

[6] Ying M., Feng Y., Yu N. Quantum Information-Flow Security: Noninterference and Access Control. [http://arxiv.org/abs/1301.6804]