СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА НА ПОСЛЕДОВАТЕЛЬНО-ПАРАЛЛЕЛЬНЫХ ГРАФАХ

В.В. Лепин

Институт математики НАН Беларуси,
Сурганова 11, 220072 Минск, Беларусь
lepin@im.bas-net.by

Неформально говоря, схема разделения секрета позволяет "распределить" информацию о сообщении S между участниками из множества $\mathcal{P}$ таким образом, чтобы заранее заданные разрешенные подмножества участников могли однозначно восстановить сообщение S, а неразрешенные — не имели такой возможности.

Защищаемое сообщение S называется *секретом*, а множество $\mathbb{S}$ всех возможных секретов — множеством секретов. Сообщение, содержащее частичную информацию о секрете и которое создано для индивидуального участника, называется *долей* этого участника. Множество всех возможных значений долей участника P обозначают через $\mathcal{S}(P)$. Для множества участников $A = \{P_{i_1}, \ldots, P_{i_r}\} \subseteq \mathcal{P}$, $i_1 < \ldots < i_r$ введем обозначение $\mathcal{S}(A) = \mathcal{S}(P_{i_1}) \times \cdots \cdots \times \mathcal{S}(P_{i_r})$.

Совокупность множеств разрешенных участников называется *структурой доступа*. Говорят, что структура доступа $\Gamma = \{A_i \in 2^P\}$, определенная на $\mathcal{P}$, является *монотонной*, если она удовлетворяет следующему условию: $A, A' \in \mathcal{P}$, $A \subseteq A'$, $A \in \Gamma \Rightarrow A' \in \Gamma$.

Монотонную структуру доступа Γ можно однозначно идентифицировать семейством ее минимальных множеств $\Gamma^- = \{A \in \Gamma : A' \not\subset A, \forall A' \in \Gamma \setminus \{A\}\}$, называемым базисом Γ.

Пара алгоритмов $\Pi = (Share, Recover)$ называется *схемой разделения секрета* для секретов из $\mathbb{S}$, если $Share$ — вероятностный алгоритм, который для входа $S \in \mathbb{S}$ вырабатывает n-мерный вектор $\mathbf{S} := {}_R Share(S)$ с элементами $\mathbf{S}[i] \in \{0,1\}^*$ и $Recover$ — детерминированный алгоритм, который для входа $\mathbf{S} \in (\{0,1\}^* \cup \{\Diamond\})^n$ вырабатывает значение $S := Recover(\mathbf{S})$, где $S \in \mathbb{S} \cup \{\perp\}$. Алгоритм $Share(S)$ выдает символ $\perp$ ("неопределенность"), если секрет не возможно реконструировать.

Любая схема разделения секрета для секретов из $\mathbb{S}$ и вероятностное распределение $\{\Pr_{\mathbb{S}}(S)\}_{S \in \mathbb{S}}$ естественным образом индуцируют вероятностное распределение $\{\Pr_{\mathcal{S}(A)}(\mathbf{x})\}_{\mathbf{x} \in \mathcal{S}(A)}$ на $\mathcal{S}(A)$ для каждого подмножества $A \subseteq \mathcal{P}$. Пусть $H(S)$ - энтропия распределения $\{\Pr_{\mathbb{S}}(S)\}_{S \in \mathbb{S}}$, а $H(A)$ — энтропия распределения $\{\Pr_{\mathcal{S}(A)}(\mathbf{x})\}_{\mathbf{x} \in \mathcal{S}(A)}$.

Схему разделения секрета называют *совершенной* на структуре доступа Γ, если для всех $A \in \Gamma$ выполняется $H(S|A) = 0$, а для всех $A \notin \Gamma$ выполняется $H(S|A) = H(S)$.

Информационным отношением совершенной схемы разделения секрета Π для секретов из $\mathbb{S}$ и структуры доступа Γ называют величину

$$\rho(\Pi, \Gamma, \mathbb{S}) = \frac{\log |\mathbb{S}|}{\max_{P \in \mathcal{P}} \log |\mathcal{S}_{\mathcal{P}}|}.$$

Оптимальным информационным отношением для структуры доступа Γ называют величину $\rho(\Gamma) = \sup \rho(\Pi, \Gamma, \mathbb{S})$.

Аналогично, *среднее информационное отношение* $\widetilde{\rho}(\Pi, \Gamma, \mathbb{S})$ определяется так:

$$\widetilde{\rho}(\Pi, \Gamma, \mathbb{S}) = \frac{|\mathcal{P}| \log |\mathbb{S}|}{\sum_{P \in \mathcal{P}} \log |\mathbb{S}_{\mathcal{P}}|},$$

а *оптимальное среднее информационное отношение* для Γ так: $\widetilde{\rho}(\Gamma) = \sup \widetilde{\rho}(\Pi, \Gamma, \mathbb{S})$.

В докладе будут представлены эффективные алгоритмы вычисления нижних и верхних оценок для оптимального и оптимального среднего информационных отношений структур доступа базисами, которых являются множества ребер последовательно-параллельных графов.

Работа выполнена при финансовой поддержке БРФФИ (проект Ф07-293).