# Схема Блома предварительного распределения ключей на эллиптических кривых для беспроводных сенсорных сетей

***Воеводин Кирилл Сергеевич***

*Студент*

*Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия*

*E-mail:* voevod_kirill@mail.ru

Безопасность в беспроводных сенсорных сетях (БСС) имеет обширную область исследования, которая довольно сильно отличается от традиционных механизмов сетевой безопасности. БСС представляет собой распределенную, самоорганизующуюся сеть множества датчиков и исполнительных устройств, объединенных между собой через радиоканал. Особенности архитектуры сенсорных сетей, такие как малое потребление энергии, масштабируемость, равнозначность узлов, одновременное функционирование большого количества узлов на ограниченном пространстве, накладывают ограничения на обеспечение их безопасности.

Основной темой исследования является протокол управления ключей в сенсорных сетях, который ввиду изложенных особенностей сенсорных сетей, должен обладать высоким уровнем безопасности и иметь низкие накладные расходы.

Для обеспечения конфиденциальности передаваемой информации между узлами используют механизм шифрования, что формирует задачу предварительного распределения ключей шифрования между узлами. Данная задача может быть решена с использованием механизмов либо открытого, либо секретного ключа.

Однако современные беспроводные динамические сети, в частности, сенсорные, состоят из большого числа узлов, обладающих слабыми вычислительными ресурсами процессора и ограниченным объемом памяти. В такой сети применение инфраструктуры открытых ключей неоправданно. Кроме того, топология динамических сетей, как правило, не известна заранее и может быть установлена только после развертывания сети.

Существует способ, более подходящий для решения проблемы распределения ключей в динамических сетях, – способ предварительного распределения ключей (СПРК). Далее предложена реализация схемы Блома предварительного распределения ключей в беспроводных сенсорных сетях, в основе которой лежит использование эллиптической криптографии. Пусть $n$ – число узлов сети. $\mathcal{E}(a, b)$ –

множество точек ЭК, являющихся решениями канонического уравнения ЭК над полем $\mathrm{F_p}$ с характеристикой $p > 3$, дополненное бесконечно удаленной точкой $\Theta$. Множество значений открытых ключей $\mathrm{R} = \{\mathrm{F_p}\}^{m+1}$. $A(\mathcal{P})$ – симметричная секретная матрица порядка $m+1$ над точкой $\mathcal{P}$ эллиптической кривой (генератор группы $\mathcal{E}(a,b)$). Тогда $A(\mathcal{P}) = \{a_{ij}^{\mathcal{P}}\}_{i=0,j=0}^{n,m} \in \mathrm{P} = \{\mathcal{E}(a,b)\}^{m+1\times m+1}$, где $a_{ij}^{\mathcal{P}} \in \mathcal{E}(a,b),\ 0 \leqslant i,j \leqslant m$. Множество значений ключевой информации $\mathrm{Q} = \{\mathcal{E}(a,b)\}^{m+1}$. Ключи множества K суть элементы группы $\mathcal{E}(a,b)$. Центр распределения ключей $C$ выбирает $n$ линейно независимых векторов из множества R вида $\vec{r}_i = (r_{i,1}, r_{i,2}, r_{i,3}, ..., r_{i,m+1}),\ 1 \leqslant i \leqslant n$, которые являются открытыми ключами узлов сети. Затем $C$ отправляет соответствующий вектор каждому абоненту сети. Линейная независимость векторов необходима для выполнения свойства $m$-стойкости схемы. $C$ передает узлу $A$ с номером $i_A$ и открытым ключом $\vec{r}_{i_A} \in \mathrm{R}$ ключевые материалы по надежному каналу, обеспечивающему конфиденциальность, определяемые следующей формулой:

$$\vec{q}_{i_A}(\mathcal{P}) = \vec{r}_{i_A} \cdot A(\mathcal{P}) = \left\{ \sum_{k=0}^{m} r_{i_A k} \cdot a_{kj}^{\mathcal{P}}, \quad 0 \leqslant j \leqslant m \right\}.$$

Для связи двух узлов $A$ и $B$ с номерами $i_A$ и $i_B$ и соответствующими открытыми ключами $\vec{r}_{i_A}$ и $\vec{r}_{i_B}$ им необходимо сгенерировать общий секретный ключ по следующей формуле:

$$k_{i_A i_B}^{\mathcal{P}} = \vec{q}_{i_A}(\mathcal{P}) \cdot (\vec{r}_{i_B})^T = \vec{r}_{i_A} \cdot A(\mathcal{P}) \cdot (\vec{r}_{i_B})^T = \sum_{l=0}^{m} \left[ \sum_{k=0}^{m} r_{i_A k} \cdot a_{kl}^{\mathcal{P}} \right] \cdot (r_{l i_B})^T.$$

Использование эллиптической криптографии обусловлено криптографической стойкостью задачи дискретного логарифмирования для групп точек эллиптических кривых (ECDLP), а также меньшими потребляемыми информационными ресурсами памяти.

**Литература**

1. Алферов А.П., Зубков А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии – М.: «Гелиос Ассоциация Российских вузов», 2002.
2. Zhang Y., Hu H., Fujise M. Resource, Mobility, and Security Management in Wireless Networks and Mobile Communications // Auerbach Publications Taylor, New York, 2006, P 445.