СХЕМА ОФЛАЙН-ГЕНЕРАЦИИ ЭФЕМЕРНЫХ КЛЮЧЕЙ ШИФРОВАНИЯ В ОДНОРАНГОВОЙ СЕТИ

Захарченко К. В., Шилин Л. Ю.
Кафедра информационных технологий автоматизированных систем, кафедра теоретических основ электротехники, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: cvzakharchenko@gmail.com

В статье предлагается возможный вариант расширения протокола Signal для выполнения в условиях отсутствия центрального сервера с сохранение свойств протокола. В частности предлагается альтернативный метод распространения эфемерных ключей шифрования, основывающийся на использовании криптографических билинейных отображений и сложности решения задачи суммы подмножества.

Введение

Во многих задачах распределённые пиринговые сети являются выгодной альтернативой клиент-серверным решениям. Причинами этому являются: отсутствие затрат на поддержку и разработку серверной части, автоматическая масштабируемость сети за счёт использования ресурсов клиентов, отсутствие единой точки отказа и прочие. Но помимо решения многих проблем клиент-серверной архитектуры, пиринговые сети также ставят перед разработчиками ряд новых задач. Так, например, при реализации распределённой системы мгновенного обмена сообщениями особой задачей стоит протокол шифрования сообщений. В клиент-серверных решениях одним из наиболее распространённых и заслуживших доверие протоколов является протокол Signal, использующийся в таких системах обмена сообщениями, как WhatsApp, Facebook Messenger, Google Allo и других [1]. Целью данной работы стоит адаптация протокола Signal к работе в условиях отсутствия центрального сервера.

I. Краткое описание протокола Signal

Протокол Signal использует 10 различных классов ключей и его описание достаточно объёмно, подробный анализ протокола представлен в литературе[1]. Список полезных свойств этого протокола включает в себя: сквозное шифрование, прямая и обратная секретность (forward and backward secrecy), генерация сессионного ключа в режиме офлайн (пользователи могут обмениваться сообщениями не присутствуя в сети одновременно). В начале выполнения протокола генерируются ассиметричные ключи 3 типов:

1. долгосрочный ключ;
2. кратковременный ключ;
3. набор эфемерных ключей.

Открытая часть долгосрочного и кратковременного ключа публикуется, закрытая часть хранится пользователем в секрете. Долгосрочный ключ используется для подписи и аутентификации как сообщений, так и кратковременных и эфемерных ключей. Кратковременный ключ используется для генерации сессионного ключа, для чего протокол Signal утилизирует метод двойного храповика (double ratchet). Эфемерные ключи используются для обеспечения дополнительных свойств безопасности и в отличие от первых двух ключей требуют особый метод публикации, реализованный на центральном сервере. Если пользователь A желает отправить сообщение пользователю B, он обращается к серверу с запросом эфемерного ключа, сервер выдаёт ключ из списка ключей пользователя B и удаляет ключ из списка. После того, как эфемерные ключи заканчиваются на сервере, они перестают использоваться в протоколе Signal и протокол теряет свойства прямой и обратной секретности.

II. Получение эфемерных ключей в распределённой сети

Протокол Signal требует, чтобы сервер, хранящий эфемерные ключи не выдавал каждый ключ более, чем одному пользователю, то есть удалял уже использованные ключи. Такая функциональность трудно реализуема в условиях одноранговой пиринговой сети без участия арбитров с особыми привилегиями. Сложно доверить пользователям распределённой сети возможность удаления чужих ключей. Поэтому в данной работе предлагается производить генерацию эфемерного ключа стороной, отправляющей сообщение, но так, чтобы только принимающая сторона могла восстановить эфемерный ключ за время полиномиально зависящее от длины ключа.

III. Используемые конструкции

Для построения целевой схемы в данной работе используются криптографические билинейные отображения и свойства NP-полной задачи суммы подмножества. Дадим краткие определения.

Пусть имеется n групп $\{H_1, ..., H_n\}$ с генераторами $G = \{g_1, ..., g_n\}$ соответственно, тогда семейство билинейных отображений на этих груп-

пах задаётся следующим образом[3]:

$$\{e_{i,j} : H_i \times H_j \to H_{i+j} | i,j \in [n]; i+j \leq n\},$$

где для каждого $e_{i,j}$ выполняется

$$e_{i,j}(g_i^a, g_j^b) = g_{i+j}^{ab} : \forall a,b \in Z_p.$$

Задача суммы подмножества, заданная множеством целых чисел $V = \{v_1, ..., v_n\} \subset Z_p$ и числом t, состоит в том, чтобы найти такое подмножество $T \subseteq V$, что $t = \sum_{v \in T} v$. Эта задача является NP-полной и на данный момент неизвестен алгоритм эффективно решающий эту задачу в общем случае[2].

IV. Схема генерации эфемерных ключей

Предлагаемая схема описана в данном разделе. Пусть в качестве открытых параметров протокола выступают: параметр k, задающий уровень безопасности системы, параметр $n = (k(k+1))/2$, задающий размер семейства билинейных отображений и семейство билинейных отображений $\{e_{i,j} | i,j \in [n]; i+j \leq n\}$.

Пользователь A, желающий получать сообщения, рандомизированным образом генерирует множество чисел $V = \{v_1, ..., v_k\} \overset{R}{\subset} Z_p$, секретный параметр $\alpha \overset{R}{\leftarrow} Z_p$ и генераторы групп $G = \{g_1, ..., g_n\}$. Далее пользователь кодирует множество V следующим образом:

$$P = \{p_1, ..., p_k\} = \{g_1^{\alpha^{v_1}}, ..., g_k^{\alpha^{v_k}}\}.$$

В качестве открытой информации протокола пользователь A публикует параметры V и P, а локально сохраняет генераторы групп G и секретный параметр α.

Пользователь B, желающий отправить сообщение пользователю A, получает из распределённой сети параметры $V = \{v_1, ..., v_k\}$ и $P = \{p_1, ..., p_k\}$. Для генерации эфемерного ключа пользователь B выбирает случайное подмножество $I = \{i_1, ..., i_m\} \overset{R}{\subseteq} [k]$ так, что $|I| \geq 2$ и вычисляет параметры:

$$kv = \sum_{i \in I} v_i,$$

$$ki = \sum_{i \in I} i,$$

$$kp = f_m(p_{i_1}, ..., p_{i_m}) = f_m(g_{i_1}^{\alpha^{v_{i_1}}}, ..., g_{i_m}^{\alpha^{v_{i_m}}}) =$$

$$= f_m(g_{i_1}, ..., g_{i_m})^{a^{v_{i_1}+\cdots+v_{i_m}}} = g_{ki}^{a^{kv}},$$

где $f_m : H_{i_1} \times ... \times H_{i_m} \to H_{ki}$ – рекурсивная функция

$$f_m(p_{i_1}, ..., p_{i_m}) =$$

$$= e_{i_1+\cdots+i_{m-1},i_m}(f_{m-1}(p_{i_1}, ..., p_{i_{m-1}}), p_{i_m}),$$

с базой рекурсии

$$f_2(p_{i_1}, p_{i_2}) = e_{i_1,i_2}(p_{i_1}, p_{i_2}).$$

Фактически функция f_m выполняет свёртку слева списка $p_{i_1}, ..., p_{i_m}$ по билинейным отображениям $e_{i,j}$.

Полученные параметры kv и ki подписываются долгосрочным ключом и пересылаются пользователю A в открытом виде через распределённую сеть, а параметр kp используется при шифровании сообщения, как эфемерный ключ.

Принимающая сторона, получив параметры kv и ki, может восстановить использованный при шифровании эфемерный ключ, так как ей известны генераторы групп и секретный параметр α. Эфемерный ключ можно вычислить как

$$kp = g_{ki}^{\alpha^{kv}}.$$

Таким образом происходит генерация и восстановление эфемерного ключа. Третья сторона C, перехватывающая данные, посылаемые по открытому каналу имеет доступ к параметрам V, P, ki и kv. Чтобы восстановить ключ kp, сторона C должна решить задачу нахождения подмножества $T \subseteq V$, для которого верно $\sum_{v \in T} v = kv$, что эквивалентно решению задачи суммы подмножества. Для решения этой задачи в общем случае (при случайно сгенерированных v_i) количество операций, которое необходимо выполнить лучшему из известных алгоритмов[2], экспоненциально зависит от размера множества V, что на практике при достаточном размере V делает задачу нерешаемой за какое-либо осмысливаемое время. Более того, даже, если третья сторона сможет решить один экземпляр задачи, это не даст ей возможность решать другие экземпляры задачи с каким-либо преимуществом, в чём и заключается эфемерность полученного ключа.

Заключение

Статья предлагает возможный вариант использования криптографических билинейных отображений для адаптации выполнения протокола Signal в условиях одноранговой сети. Преимущество предложенной схемы заключается в отсутствии необходимости в арбитраже со стороны центрального сервера. Недостатки отражаются в увеличении сложности протокола и объёма вычислений. Предложенная схема основывается на трудности решения NP-полной задачи. Поэтому злонамеренная сторона может рассекретить сгенерированный эфемерный ключ, но для этого ей понадобится огромное количество вычислительных ресурсов, экспоненциально зависящее от длины ключа. Дальнейшую работу следует направить на изучение точных временных затрат, связанных с выполнением протокола, объёма передаваемых через распределённую сеть данных и на тщательный анализ параметров безопасности предложенной схемы.

1. Cohn-Gordon K. et al. A formal security analysis of the signal messaging protocol //Security and Privacy (EuroS&P), 2017 IEEE European Symposium on. – IEEE, 2017. – С. 451-466.
2. Cormen T. H. et al. Introduction to algorithms. – MIT press, 2009. – С. 1128-1133
3. Boneh D., Franklin M. Identity-based encryption from the Weil pairing //Annual international cryptology conference. – Springer, Berlin, Heidelberg, 2001. – С. 213-229.