И.Д. Трацевский, О.В. Ниссенбаум, М.Б. Атманских

Тюменский государственный университет, г.Тюмень

УДК 004.056.5

ЗАБЫВЧИВАЯ ПЕРЕДАЧА И РАСШИРЕНАЯ ЗАБЫВЧИВАЯ ПЕРЕДАЧА ДАННЫХ

Аннотация. Статья посвящена разработке учебно-методического наполнения для курса "Криптографические протоколы" по теме "Забывчивая передача". Этот класс протоколов является основой развивающегося раздела конфиденциальных вычислений и практически не представлен в русскоязычной литературе. В статье описаны избранные протоколы забывчивой передачи и их расширения, подходящие для освоения студентами, определены темы лабораторных работ.

Ключевые слова: забывчивая передача, расширенная забывчивая передача, протоколы.

Введение

Забывчивая передача (англ. ObliviousTransfer, далее - OT) является основой для протоколов двухсторонних и многосторонних конфиденциальных вычислений, протоколов пересечения частных множеств, и других задач современной прикладной криптографии. Постоянно разрабатываются новые протоколы OT с улучшенными свойствами эффективности и безопасности.

Поскольку проблемы конфиденциальных вычислений, связанных с проведением электронных выборов и аукционов, осуществлением запросов к частным базам данных, становятся все более актуальными, необходимость в забывчивых протоколах передачи данных становится все более очевидна. Однако, в большинстве случаев, в современных

протоколах конфиденциальных вычислений запускаются миллионы забывчивых передач, что становится излишне вычислительно дорого. Для решения этой проблемы и разрабатываются протоколы расширенной забывчивой передачи данных (англ. Oblivious Transfer extensions, далее - OTe).

Протоколы забывчивой передачи нашли широкое применение в современной криптографии: их используют в обмене ключей [1], общих многосторонних вычислениях, искаженных схемах Яо и других задачах современной прикладной криптографии. Постоянно появляются новые и совершенствуются старые протоколы OT [2];[3] и OTe [4].

Целью данной работы является исследование протоколов OT и их расширений – OTe, а также разработка учебно-методического пособия по теме «Забывчивая передача».

Протокол забывчивой передачи

Протокол забывчивой передачи был впервые представлен М. Рабиным в 1981 году [5], и включал в себя двух участников – отправителя и получателя. В наиболее часто используемой версии протокола - 1 из 2-х, отправитель обладает парой сообщений (m_0,m_1), а получатель обладает битом выбора r. По окончании протокола, получатель обладает сообщением m_r (но не знает ничего о другом сообщении), а отправитель не узнает ничего об r.

Существуют также версии протокола 1-из-n, в которых на выбор дается n различных сообщений, а получатель должен выбрать только одно из них ик-из-n, где получатель выбирает k сообщений из n. Обе версии являются обобщением протокола 1 из 2-х.

Моделирование противника

Чаще всего выделяют два типа противников:

- Пассивный – следует протоколу, но пытается выяснить больше, чем положено протоколом.

- Активный – следует любой выбранной для себя стратегии в попытке нарушить выполнение протокола. Очевидно, что сложнее всего защититься именно от активного противника.

Однако существует также понятие скрывающегося противника, которого считают ближе к реальному миру, чем просто активного [6]. Скрытый противник — это активный противник, который также следует любой стратегии, но стремится не быть разоблаченным.

Идеальная модель

Идеальная модель, или модель идеального мира – это использование промежуточной системы, которая получит пару сообщений (m_0,m_1) от отправителя и бит выбора r от получателя и отправит m_r получателю. Очевидно, что в реальном мире такая система не гарантирует безопасности и не используется, поскольку злоумышленником может оказаться именно промежуточная система.

Забывчивая передача 1 из 2-х

Приведем пример одного из ОТ протоколов, а именно 1 из 2-х протокол Эвена, Гольдрайха и Лемпеля [7].

Отправитель обладает сообщениями m_0 и m_1 и хочет быть уверен, что получатель получит только одно из сообщений. Получатель обладает битом выбора r и хочет получить сообщение m_r так, чтобы отправитель не узнал r

Предварительные вычисления:

Отправитель генерирует пару RSA ключей, содержащих модуль N, открытый показатель степени e и закрытый показатель степени d. Также генерируются два случайных числа x_0 и x_1.

Передача:

Отправитель передает N, e, x_0и x_1получателю.

Получатель генерирует бит r и выбирает x_r. После этого он генерирует случайное k и прячет x_r , подсчитав $v = (x_b + k^e) mod N$ и передает v отправителю.

Отправитель может подсчитать два возможных k: $k_0 = (v - x_0)^d mod N$ и $k_1 = (v - x_1)^d mod N$, но не может определить какое из них верно. Заметим, что одно из этих k окажется случайным числом. Отправитель подсчитывает: $n_0 = m_0 + k_0$ и $n_1 = m_1 + k_1$ и отправляет n_0 и n_1 получателю.

Получатель знает, какое из сообщений должно быть расшифровано, поэтому он подсчитывает $m_r = n_r - k$ получая только одно сообщение от отправителя. Второе сообщение он расшифровать не сможет, т. к. оно сложено со случайным числом.

Расширенный протокол забывчивой передачи

Использование ОТ в протоколах конфиденциального вычисления, в большинстве случаев, означает необходимость в миллионах забывчивых передач, что может занимать десятки минут. Для решения этой проблемы, в 1996 году Д. Бивер впервые представил протокол расширенной забывчивой передачи. [8]

ОТе работает посредством запуска малого числа базовых ОТ, в зависимости от необходимых параметров безопасности. Эти базовые ОТ используются для выполнения большого числа забывчивых передач, через использование только дешевых, симметричных криптографических операций.

Но развитие ОТе не остановилось, криптографическая оптимизация и развитие новых алгоритмов привело к тому, что проблемой забывчивых передач с защитой от пассивного противника стала не дороговизна вычислений, а недостаточная пропускная способность канала. К примеру, для вычисления десяти миллионов забывчивых передач, через LAN с четырьмя потоками, потребовалось 2,62 секунды. [9]

Использование OTe на примере протокола IKNP с защитой от пассивного противника

Отправитель имеет m пар сообщений $(x_1^0, x_1^1), \ldots, (x_m^0, x_m^1)$

Получатель делает выбор $\sigma = \sigma_1, \ldots, \sigma_m$

Первая фаза:

Получатель подготавливает случайные строки $T_1, \ldots, T_n$ длины m, а также пары $(T_i, T_i \oplus \sigma)$. В забывчивой передаче он будет играть отправителя.

Отправитель выбирает случайное $s = s_1, \ldots, s_n$. В забывчивой передаче он будет играть получателя. Процесс обмена матрицами представлен на рисунке 1.

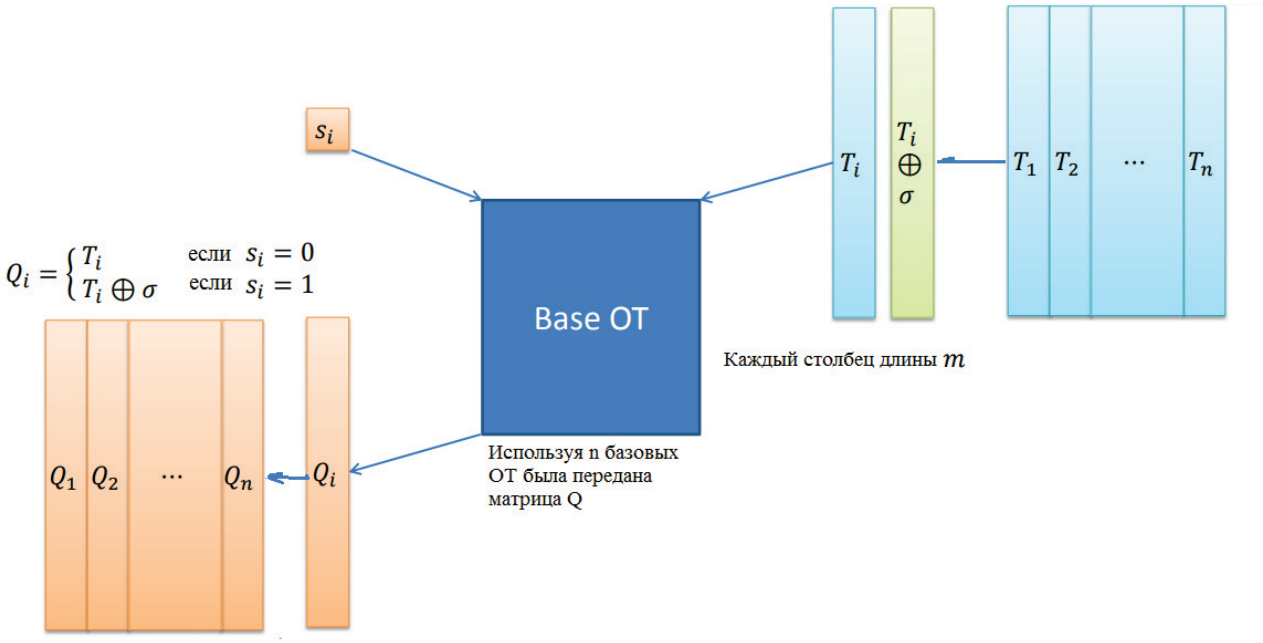

*Рис. 1.*Схема обмена матрицами в протоколе IKNP.

Используя n базовых OT матрица была передана. Теперь взглянем на строки получившихся матриц и заметим, что если $\sigma_i = 0$, тогда $T(i) = Q(i)$, иначе $T(i) = Q(i) \oplus s$.

Затем отправитель передает $y_i^0 = H\big(i, Q(i)\big) \oplus \mathrm{x_i^0}$ и $y_i^1 = H(i, Q(i) \oplus \mathrm{s}) \oplus \mathrm{x_i^1}$. Протокол заканчивается, когда получатель подсчитывает: $x_i^{\sigma_i} = H\big(i, T(i)\big) \oplus \mathrm{y_i^\sigma}$.

Возможные задачи для обучения

- Реализация OT протоколов 1 из 2-х
- Конвертация из OT протокола 1 из 2-х в 1-из-n или k-из-n.
- Сравнение скорости вычисления OT 1 из 2-х с 1-из-n и k-из-n
- Сравнение скорости вычисления OT с защитой от пассивного противника со скоростью вычисления OT с защитой от активного противника.

Заключение

Был рассмотрен тип протокола OT и его расширение – OTe, определено возможное поведение противника. Также была рассмотрена разница в скорости работы OT и OTe и составлен список задач для обучения.

СПИСОК ЛИТЕРАТУРЫ

1. Branco P., Ding J., Goulao M., Mateus P. A Framework for Universally Composable Oblivious Transfer from One-Round Key-Exchange // IMA International Conference on Cryptography and Coding, 2019. pp. 78-101.
2. Goyal V., Jain A., Jin Z., Malavolta G. Statistical Zaps and New Oblivious Transfer Protocols // Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2020. pp. 668-699.

3. Masny D., Rindal P. Endemic Oblivious Transfer // Conference on Computer and Communications Security (CCS '19), 2019. pp. 309–326.

4. Boyle E., Couteau G., Gilboa N., Ishai Y., Kohl L., Rindal P., Scholl P. Efficient Two-Round OT Extension and Silent Non-Interactive Secure Computation // Conference on Computer and Communications Security (CCS '19), 2019. pp 291–308.

5. Rabin M. O. How to exchange secrets with oblivious transfer, TR-81 edition. Aiken Computation Lab, Harvard University, 1981. 21 p.

6. Aumann Y., Lindell Y. Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries // Theory of Cryptography Conference, 2009. pp 137-156.

7. Even S., Goldreich O., Lempel A. A Randomized protocol for signing contracts // Communications of the ACM, Volume 28, Issue 6, 1985. pp. 637–647.

8. Beaver D. Correlated pseudo randomness and the complexity of private computations // Symposium on the Theory of Computing (STOC’96), ACM, 1996.pp. 479–488.

9. Asharov G., Lindell Y., Schneider T., Zohner M. More efficient oblivious transfer and extensions for faster secure computation // ACM Computer and Communications Security (CCS’13), ACM, 2013. pp. 535–548.