Онлайн атака на гвантовые деньги.

Квантовые деньги, созданные Визнером [5] - это простой пример, информационно теоретической защиты шифровального квантового протокола. Благодаря этому протоколу, монетный двор выпускает квантовые банкноты и любой может запросить у монетного двора проверку подлинности банкнот.

Протокол может быть сломан в линейном времени, если, при запросе проверки подлинности банкнот, монетный двор возвращает подделку.

Вступление.

В теории сопряженного кодирования[5] Визнера, предложено использовать в протоколе индивидуальные ключи для информационно теоретической защиты квантовых денег. Монетный двор (центральный банк) может выбрать n-параметр безопасности и произвести (генерировать) случайное значение n-кубита. Каждый кубит независим. Базисом пространства кубитов является множество $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Монетный двор присваивает банкноте код, который характеризуется уникальный серийным номером. Для верификации квантовой банкноты, торговец направляет банкноту обратно в монетный двор. Монетный двор сопоставляет набор признаков, соответствующих серийному номеру и квантовая банкнота проходит проверку.

Если результат «ДЕЙСТВИТЕЛЬНА» (состояние прошедшее тест, соответствующее описанию), это означает, что банкнота настоящая, если результат «НЕДЕЙСТВАТЕЛЬНА» это означает, что банкнота поддельная или поврежденная. (Монетному двору необходимо поддержание защищенной базы данных случайных состояний, соответствующих серийным номерам).

Этот протокол является информационно-теоретической защитой. Из теоремы о запрете клонирования следует, что нападающий, не может в точности копировать квантовую банкноту[1]. Оценки в [1] показывают, что вероятность совпадения убывает экспоненциально как функция n.

Существует много новых исследований, основанных на идее нападения на классическую систему криптографических протоколов другими способами с помощью различных каналов и web-атак. К примеру, широко используемый симметричный шифр CBC можно атаковать несколькими запросами оракула, отличающего действительные зашифрованные сообщения, от нерабочих сообщений с определенным типом ошибки [5]. Ученые эффектно продемонстрировали, что эти нападения срабатывали против небрежно разработанных web-сайтов и что много других web-сайтов уязвимы [4]. Использование этих результатов ученых

показывает, что даже если у центрального банка есть прекрасный квантовый компьютер, квантовые деньги уязвимы. Если при запросе проверки любой банкноты, монетный двор вернет банкноту, даже если банкнота была поддельной, то небольшое количество повторных запросов могут быть использованы для копирования банкноты. Для использования квантовых денег монетный двор должен создать службу, где каждый сможет проверить квантовые деньги. Если коммерсант посылает в монетный двор квантовую банкноту, то монетный двор либо отвечает, что банкнота подлинная, и возвращает банкноту, либо отвечает, что она подделана. В случае если банкнота подлинная, монетный двор уничтожит фальшивую банкноту. Если же монетный двор вернет фальшивую банкноту, тогда весь протокол может быть нарушен. Можно представить квантовую банкноту как пару классического номера и квантового состояния $(s, |\$_s\rangle)$, где s – уникальный классический серийный номер и $|\$_s\rangle$ - случайно созданное монетным двором состояние, соответствующее серийному номеру s.

Можно записать:

$$|\$_s\rangle = |\psi_1\rangle|\psi_2\rangle \dots |\psi_n\rangle,$$

где каждый вектор $|\psi_i\rangle$ пространства Гильберта зависит от s и образуется из векторов базиса $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. этого пространства. Каждое $|\psi_i\rangle$ - это собственный вектор, то есть состояние операторов X или Z. Неизвестно какому оператору соответствует собственное состояние $|\psi_i\rangle$. Предполагается, что можно отправить в монетный двор любое c-q значение $(s, |\phi\rangle)$ и монетный двор сравнит проекционным способом $P_s = |\$_s\rangle\langle\$_s|$. При результате равном 1, монетный двор покажет $(\textit{ДЕЙСТВИТЕЛЬНА}, s, P_s, |\phi\rangle)$, при результате равном 0, монетный двор выдаст $(\textit{НЕДЕЙСТВИТЕЛЬНА}, s, (1 - P_s), |\phi\rangle)$ (с точностью до нормы). Предположим, что фальшивомонетчик имеет одну квантовую банкноту $(s, |\$_s\rangle)$ и может послать запрос в монетный двор, тогда он может взломать протокол, узнав состояние одного кубита $|\$_s\rangle$ в данный момент времени. Чтобы узнать состояние i-го кубита, он посылает в монетный двор значение $(s, X_i, |\$_s\rangle)$. Если монетный двор определит, что квантовая банкнота подделана, тогда состояние, соответствующее $|\psi_i\rangle$, будет $|0\rangle$или $|1\rangle$ как и другие возможности $|+\rangle$ или $|-\rangle$), имеющиеся как собственные состояния X_i.

В случае возврата банкноты, математическое выражение будет выглядеть так:

$$|\psi_1\rangle \dots |\psi_{i-1}\rangle \left|\psi_i^{\perp}\right\rangle \left|\psi_{i+1}\right\rangle \dots |\psi_n\rangle$$

Но сейчас фальшивомонетчик знает, что $|\psi_i^{\perp}\rangle$ это собственное значение зависит от Z. Она использует X_i , чтобы получить $|\$_s\rangle$ в базисе Z, что бы узнать, является ли $|\psi_1\rangle$ - значение $|0\rangle$ или $|1\rangle$. Если же монетный двор скажет, что банкнота ДЕЙСТВИТЕЛЬНА, то тогда значение $|\psi_i\rangle$ было бы или $|-\rangle$, или $|+\rangle$. В этом случае монетный двор вернет не уничтоженное значение $|\$_s\rangle$ Карле. Но Карла знает, что $|\psi_i\rangle$ - значение имеет собственное значение от X и она может узнать, является ли это значение $|-\rangle$ или $|+\rangle$. Если повторить эти действия, i=1, … n, можно узнать секретное значение $|\$_s\rangle$ с точностью до n. Выполнив вышеописанные действия, можно изготовить несколько поддельных копий. Используют более общий алгоритм квантовой реконструкции, чтобы скопировать значение 2n (предполагаемое), запрашиваемое у монетного двора или одну томографическую копию, что бы узнать какое из запрашиваемых значений равно 0 (n) [3]. Тот, кто использует классические криптографические протоколы, должен быть очень осторожен, нужно избегать ошибок в начале, тогда защита будет блокирована, если протокол будет реализован правильно. Квантовая криптография не самая эффективная защита.

Литература

1. S. Wiesner. Conjugate coding. SIGACT News, 15(1):78–88, 1983.
2. V. Bužek, M. Hillery. Quantum copying: Beyond the no-cloning theorem. Physical Review A, 54(3):1844–1852, 1996.
3. E. Farhi et al. Quantum state restoration and single-copy tomography. 2009, arXiv:0912.3823v1.
4. J. Rizoo, T. Duong. Practical Padding Oracle Attacks. In 4th USENIX Workshop on Offensive Technologies, 2010.
5. S. Vaudenay. Security Flaws Induced by CBC Padding–Applications to SSL, IPSEC, WTLS... In EUROCRYPT 2002, pages 534–545. Springer, 2002.
6. A. Lutomirski. An online attack against Wiesner’s quantum money. http://arxiv.org/abs/1010.0256v1
7. Е. Румянцева, Р. Старобогатов. Квантовые компьютеры. «Информационные системы и технологии» Сб. научно-технических статей№1(2) РГПУ им. А.И.Герцена. СПб. 2010, с.110-115.
8. А. Балонишников, Р. Старобогатов. Квантовые модели безопасных протоколов. Вестник ИНЖЭКОНА, серия: технические науки, 2011, Вып.8(51), с.17-26.
9. Р. Старобогатов. Квантовые протоколы платежей. Вестник ИНЖЭКОНА, серия: экономические науки, 2011, в.3(46), с.138-143.

10.
11.
12.