Архитектуры безопасности в системах цифровой экономики

В. О. Писковский, А. А. Грушо, М. И. Забежайло, А. В. Николаев,
В. В. Сенчило, Е. Е. Тимонина

***Аннотация* — В работе рассматривается задача защиты информации при использовании противником методов сбора ценной информации по косвенным признакам в информационной среде, которая доступна злоумышленникам. При этом предполагается, что все персональные данные в рассматриваемом информационном пространстве обезличены. Однако обычно этих мер недостаточно. Используя информационные связи, удается преодолеть обезличивание данных, а также восстанавливать другую ценную информацию о деятельности участников экономической деятельности в цифровой экономике. Для решения задачи выявления злоумышленников, добывающих информацию по косвенным признакам, необходимы средства регистрации субъектов, организаций и частных лиц, осуществивших доступ к тем или иным данным, возможно содержащим косвенные признаки ценной информации. Данные регистрации фактов доступа должны быть доступны на публичном ресурсе. При необходимости, средство регистрации должно позволить авторизованным пользователям или комиссии, состоящей из таких пользователей, получить персональные данные организаций и лиц, осуществивших доступ к данным. Цель такого журнала регистрации фактов доступа – предоставление услуг по получению исчерпывающей и достоверной информации о том, кто, когда и в какой мере осуществлял доступ к персональным или корпоративным данным, обрабатываемым в рамках цифровой экономики. Для решения задачи предложено использовать архитектуру распределенного реестра. Эта архитектура позволяет открыто хранить данные обо всех обращениях к обезличенным базам, содержащим косвенную информацию о ценных данных. Защищенный анализ распределенного реестра позволяет выявить пользователей, которые пытаются восстановить ценную информацию по косвенным признакам. В настоящее время для реализации таких решений готова техническая и теоретическая база. В статье приведены основные компоненты для подобных решений.**

***Ключевые слова* — информационная безопасность, защита ценной информации от компрометации по косвенным признакам, распределенный реестр.**

I. Введение

В эпоху ЦЭ особую ценность приобретают данные. Цифровая идентификация личности, медицинские данные пациентов, данные учёта использования услуг операторов связи, профиль действий пользователей в интернете, профиль финансовых операций организации легко становятся объектом торговли (см., например, [1]). Независимо от цели продажи и покупки этих данных, всегда найдутся примеры нечистоплотного их использования: от откровенно злонамеренного использования поддельной цифровой идентификации и шантажа до практически легальных способов определения кредитных скоринговых баллов параметров кредитного договора физического лица или компании, не говоря уже о мошеннических телефонных звонках, рассылках электронной корреспонденции, фишинговых атаках и прочих «прелестей» раннего этапа развития «цифровой экономики».

Принципиальная проблема этих «трудностей роста» в том, что даже после проведения процедур так называемого обезличивания, анонимизации или обфускации данных истинные владельцы данных могут быть сравнительно легко восстановлены по косвенным данным. Если речь идёт о человеке, то это могут быть факты биографии, профиль его звонков, контактов в социальных сетях, почтовых рассылок, набор, порядок, преференции при посещении интернет ресурсов. Если анализируются данные юридических лиц, то профиль их банковских операций и раньше сведущим людям не давал повода усомниться, какой компании они принадлежат.

При нынешнем развитии технологий агрегации и анализа данных, идентифицировать владельца того или иного цифрового профиля представляет всё меньше труда, и чем больше данных подвергается машинному анализу, тем легче и точнее решается задача идентификации по имеющимся данным, доступнее и дешевле становится чувствительная для человека или компании информация. Иными словами, особенность информации с одной стороны состоит в том, что даже обезличенные данные обладают своей спецификой. А с другой стороны по специфике цифрового профиля субъекта, как уже было сказано, можно с достаточно

Статья получена 21 июля 2020.

Работа частично поддержана РФФИ (проекты 18-29-03081 мк, 18-29-03124 мк, 18-29-16145 мк)

В. О. Писковский, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, Россия (e-mail: vpvp80@yandex.ru).

А. А. Грушо, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, Россия (e-mail: grusho@yandex.ru).

М. И. Забежайло, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, Россия (e-mail: m.zabezhailo@yandex.ru).

А. В. Николаев, Институт химической физики им. Н. Н. Семенова Российской академии наук, Москва, Россия (e-mail: gentoorion@mail.ru).

В. В. Сенчило, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, Россия (e-mail: volodias@mail.ru).

Е. Е. Тимонина, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, Россия (e-mail: eltimon@yandex.ru).

высокой вероятностью идентифицировать его обладателя.

Задача защиты информации при использовании злоумышленником, или противником, методов сбора ценной информации по косвенным признакам рассматривалась в научной литературе [2, 3]. В частности, для такой защиты необходимо априори идентифицировать данные, которые в совокупности могут определить ценную информацию с достаточной для атакующей стороны точностью. При этом надо учитывать, что такие данные остаются в публичном информационном пространстве и доступны мошенникам. Если идентифицированы источники косвенных данных, то повышенный интерес к этим источникам может компрометировать злоумышленника. Поэтому, запоминая информацию об обращениях к источникам косвенных данных, можно суммировать эти данные и не только идентифицировать злоумышленника, но также собрать доказательную базу его обвинения.

II. Пример

Очевидно, что для лечения большинства болезней необходимо собирать и использовать опыт, накопленный другими врачами в различных клиниках. Проблема объединенного использования медицинских баз данных обсуждалась на многих конференциях и в многочисленных публикациях. Для защиты персональных данных при врачебном обмене опытом используется обезличивание. Однако выше отмечалось, что при злом умысле преодоление такой защиты возможно. Давно известен метод использования функциональных зависимостей в базах данных [4, 5]. Для использования метода функциональных зависимостей необходимо делать множественные, специальным образом созданные запросы в базу данных. Причем в этих запросах интересующая противника ценная информация прямо не указывается. Вместе с тем суммирование результатов запросов дают возможность однозначно определять диагноз конкретного пациента и другие ценные данные. Если запомнить последовательность и содержание сделанных запросов, то можно идентифицировать противника и его цели. Отметим, что противник может использовать все базы данных различных клиник, прикрываясь благородными целями**.**

Контроль за сбором косвенных признаков будет атаковаться противником. Поэтому база данных обращений должна быть защищена. Проблема усложняется тем, что эта база должна быть распределенной, то есть собираться в разных организациях. Наиболее важным аспектом является защита целостности и упорядоченности таких данных. Кроме того, злоумышленник априори не известен, поэтому необходимо помнить обращения всех пользователей. Конфиденциальность требуется для защиты аналитики собранных данных. Существенным требованием является объем хранимой информации и скорость сбора данных. Необходимо учитывать, что распределенные баз данных потребуется интегрировать, чтобы иметь возможность вести анализ по многим пользователям.

III. Предложения по техническим решениям

Сформулируем требования к такому средству регистрации фактов доступа:

1) децентрализация доступа, хранения и учета, отсутствие логического центра управления
2) исключение фактов фальсификации регистрируемой информации
3) возможность деанонимизации хранимой журнальной информации должна быть только у собрания представителей коллегиального органа, обладающего соответствующими полномочиями, минимальное количество таких представителей регулируется соглашением,
4) возможность для владельцев информации получить данные о наличии фактов и времени доступа к охраняемым данным.

Требованиям 1) и 2) удовлетворяют системы распределенного реестра (Distributed Ledger Technology – DLT далее). Выполнение требований 3) и 4) может быть реализовано также применением в DLT системах ряда разработок в области криптографии: доказательство с нулевым разглашением [4], пороговая подпись [6]. Как показала практика, применение указанных технологий требует тщательного теоретического рассмотрения на предмет не только выполнения требований, но и доказательства стойкости алгоритмов и принципиального отсутствия технических возможностей компрометации применяемых методов [7].

Как упоминалось выше, для решения задачи целесообразно использование технологии распределенных реестров. Рассмотрим используемые на сегодняшний день разработки в части DLT

A. Блокчейн

Блокчейн (Blockchain) – связный список элементов, называемых блоками, в идейном плане – это основа DLT. В общем виде этот метод реализует hash дерево Меркля [8, 9]. Каждый блок содержат полезную информацию, например, содержание сообщения с изложением, вопроса и вариантов ответа или собственно информация о сделанном выборе. Собственно, ради регистрации этой информации и создается очередной элемент в цепи блоков.

Хеш-функция

Hash-функции являются главным инструментом обеспечения безопасности DLT. Блок также содержит число, временную метку, собственную контрольную hash-сумму, и hash-сумму предыдущего блока. Для подсчета контрольной суммы используется один из алгоритмов hash-функций. Смысл такого подхода - в стойкости и скорости работы, которые предъявляются к hash-функциям [10].

Наиболее используемые хеш-функции: MD5, SHA-1, SHA-256, в России – ГОСТ Р 34.11-2012 (Стрибог).

Для изменения содержимого блока придется после внесения изменений не только пересчитать его собственную контрольную сумму, но и сумму блока, который на него ссылается, и так далее, до последнего на текущий момент блока в цепочке.

Для регистрации блоков применяется технология распределенного консенсуса DLT, когда блоки и их

точные копии хранятся на множестве разных компьютеров, принадлежащих независимым друг от друга владельцам.

В некоторых типах DLT, например, распределенном реестре транзакций BitCoin, чтобы сделать описанный выше процесс изменения исторических данных ещё более затруднительным, а по сути, исключить такую возможность, использован метод, изначально созданный для ограничения количества спама и количества DoS атак. Метод состоит в использовании системы «доказательства правильности работы». В случае электронной почты, это – наличие нулей в первых 20 битах при 160 битной длине самого значения hash-функции. Реализация в случае BitCoin в отличие от реализации в электронной почте накладывает более жёсткие ограничения на значение hash-функции, которая должна быть меньше некоторой константы. Величина этой константы изменяется в зависимости от текущей скорости вычисления с целью контролировать скорость появления новых блоков в распределенном реестре, что зависит от затраченных для этого вычислительных ресурсов.

Идентификация

Для идентификации учётных записей распределенного реестра используется система Диффи-Хеллмана распределения открытых криптографических ключей – математически связанных ключевых пар. Блок подписывается секретной частью ключа, идентификация подписи осуществляется открытой частью. Подделка подписи относится к разряду NP-сложных задач дискретного логарифмирования над конечным полем [4]. Хранение секретной части ключа не допускается на недоверенных устройствах. Как следствие, подпись секретной частью владельца учётной записи допускается исключительно на устройстве, полностью контролируемым владельцем, включая интерфейсы с другими устройствами.

Децентрализация

В основе DLT лежит децентрализация хранения информации [11]. Для поддержания ссылочной целостности используется один из протоколов BitTorrent, разработанных для распределенного хранения и обмена информацией (файлами) в одноранговой сети.

Задача прозрачности и корректности данных, при условии полного согласованного контроля внесения изменений в реестр, решается набором технологий фиксации транзакций. Процесс регистрация транзакций по изменению DLT зависит от модели DLT и протокола достижения консенсуса.

Производительность

Для реализации рассматриваемых журнальных систем необходимо обеспечить крайне высокую производительность. Производительность такой системы для регистрации фактов доступа зависит от количества регистрируемых фактов в секунду, должна быть хорошо масштабируема и расширяема. В среднем банке производительность такой системы должна оцениваться в тысячи транзакций в секунду (TPS) и быть хорошо масштабируема. Для примера, пропускная способность сети SWIFT – 50 тысяч TPS, Visa – 45 - 65 тысяч TPS [12, 13].

Система журналирования должна хранить обезличенные данные, идентификационные номера участников транзакция, по которым восстановить владельцев не представляется технически возможным. В силу этого такая система может быть открыта и объединять журналы нескольких операторов персональных данных без риска непосредственной компрометации.

B. HashGraph

HashGraph, хешграф – направленный ациклический граф, каждый узел хранит свою историю "событий" (аналогов блоков в блокчейне) и обменивается информацией по определенному протоколу "слухов" (gossip protocol). Запатентованный протокол обеспечивает высокую масштабируемость при условии сохранения надёжности [14].

C. Holochain

Модель Holochain [15], по мнению её разработчиков, представляет отдельную ветвь DLT. Платформа Holochain состоит из сети агентов, поддерживающих уникальную цепочку источников своих транзакций, в сочетании с общим пространством, реализованным в виде проверочной, монотонной, сегментированной, распределенной хеш-таблицы (DHT), где каждый узел применяет правила проверки для этого данные в DHT, а также данные о происхождении данных из исходных цепочек, в которых они возникли. По мнению разработчиков Holochain, платформа поддерживает системную целостность без введения консенсуса. Holochain, также, как и Hedera (HashGraph) использует gossip protocol для узлов, чтобы поделиться информацией о обственном опыте поведения других узлов.

D. DAG

DAG - направленный ациклический граф, хорошо масштабируемая альтернатива блокчейнам для построения DLT.

Отметим что, метод HashGraph, хешграф – это DAG.

DAG является также самостоятельным методом DLT [16]. Любой узел в одноранговой сети может, как проверять, так и создавать сообщения, содержащие регистрируемую в реестре информацию. В отличие от HashGraph, все узлы в DAG выполняют двойную функцию: не только проверку, но и представление проверенной транзакции.

В blockDAG каждая вершина содержит набор транзакций, который похож на концепцию блока в блокчейне. Что отличает blockDAG от blockchain, так это то, что каждый блок может быть хеш-ориентирован на несколько родительских блоков.

В отличие от blockDAG, в txDAG каждая вершина графа представляет уникальную транзакцию, а расходящиеся ветви вершины должны содержать непересекающиеся транзакции. Это удобно для разрешения конфликтов, следовательно, такая сеть менее требовательна к вычислениям на узлах, что, в свою очередь, позволяет повысить производительность реестра, ограниченную только пропускной способностью сети.

IV. Алгоритмы достижения консенсуса в DLT

Однако, наибольшее влияние на производительность систем DLT оказывает применяемый алгоритм достижения консенсуса [11, 17].

Остановимся на определении консенсуса, как процедуры принятия решения. Технические устройства для поддержки согласованного состояния объекта, распределенного по нескольким устройствам, используют протоколы и алгоритмы согласования, набор математических правил и функций, позволяющих обеспечить работоспособность такого объекта. Разработка и обоснование этих протоколов – предмет исследования серьёзных математических дисциплин, и даже небольшое улучшение показателей в этой области приносит большие дивиденды в реализации тех или иных технических решений, от хранения данных до навигации космических аппаратов. С развитием распределенных реестров повышенное внимание было привлечено к исследованию протоколов консенсуса. Анализу протоколов консенсуса авторы собираются посвятить одну из своих следующих статей.

Для целей рассматриваемой в статье задачи, консенсус необходим для создания объединенной базы данных-хранилища доступов, децентрализованной и распределенной, которая хранится у всех участников консорциума.

V. Заключение

В работе предложен новый подход к защите ценной информации в открытом информационном пространстве. Этот подход основан на идеи, аналогичной компьютерному аудиту, который изложен еще в [18], основанный на ответственности за нарушение правил информационной безопасности. В публичном информационном пространстве целесообразно базу данных отслеживания доступов пользователей к распределенной базе строить на основе DLT. В работе рассмотрены различные технологии для реализации таких решений.

Библиография

[1] BL и Big Data: Обзор TAdviser [Online]. Available: https://www.tadviser.ru/index.php/BI.

[2] A. A. Grusho, N. A. Grusho, M. I. Zabezhailo, E. E. Timonina, “Protection of valuable information in public information space,” *Communications of the ECMS. Proceedings of the 33th European Conference on Modelling and Simulation*, vol. 33, no. 1, pp. 451–455, 2019.

[3] А. А. Грушо, Н. А. Грушо, М. И. Забежайло, Е. Е. Тимонина. “Защита ценной информации в информационных технологиях,” *Проблемы информационной безопасности. Компьютерные системы*, № 2. С. 22-26, 2018.

[4] Грушо А.А., Применко Э.А., Тимонина Е.Е. *Теоретические основы компьютерной безопасности*, М.: Академия, 2009.

[5] Su, Tzong-An and Gultekin Özsoyoglu. “Data Dependencies and Inference Control in Multilevel Relational Database Systems,” in *1987 IEEE Symposium on Security and Privacy*, pp. 202-202, 1987.

[6] C. Stathakopoulou, C. Cachin, “Threshold Signatures for Blockchain Systems,” Zurich: IBM Research, 2017. Available: https://pdfs.semanticscholar.org/2300/3bfc73e8d2fde9a465f4054f55ad1f2e8113.pdf?_ga=2.94560920.504720217.1596215569-1669259798.1588171840.

[7] Leemon Baird, “The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance,” 2016. Available: https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf.

[8] Merkle Tree. [Online]. Available: https://en.wikipedia.org/wiki/Merkle_tree.

[9] Georg Becker, “Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis,” 2008. [Online]. Available: https://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/becker_1.pdf.

[10] Rajeev Sobti, G.Geetha, “Cryptographic Hash Functions: A Review”, *International Journal of Computer Science Issues*, vol. 9, issue 2, no 2, pp. 461-479, 2012. Available: https://www.researchgate.net/publication/267422045_Cryptographic_Hash_Functions_A_Review.

[11] Anton Churyumov, “Byteball: A Decentralized System for Storage and Transfer of Value,” [Online]. Available: https://obyte.org/Byteball.pdf.

[12] Bjorn Hauge,” SWIFTNet, VisaNet and Blockchain: The Future of Clearing,” 2018, [Online]. Available: https://medium.com/datadriveninvestor/swiftnet-visanet-and-blockchain-the-future-of-clearing-f42de3ced34c.

[13] VISA, [Online]. Available: https://usa.visa.com/partner-with-us/payment-technology/visa-b2b-connect.html.

[14] Dr. Leemon Baird, Mance Harmon, and Paul Madsen, “Hedera: A Public Hashgraph. Network & Governing Council. The trust layer of the internet,” 2019. [Online]. Available: https://www.hedera.com/hh-whitepaper-v1.4-181017.pdf.

[15] Eric Harris-Braun, Nicolas Luck, Arthur Brock, “Holochain. Scalable agent-centric distributed computing,” DRAFT (ALPHA 1) - 2/15/2018. [Online]. Available: https://whitepaperdatabase.com/wp-content/uploads/2018/08/holochain-HOT-whitepaper.pdf.

[16] Directed Acyclic Graphs (DAGs). [Online]. Available: https://ericsink.com/vcbe/html/directed_acyclic_graphs.html.

[17] Tai-Yuan Chen, Wei-Ning Huang, Po-Chun Kuo, Hao Chung and Tzu-Wei Chao, “A Highly Scalable, Decentralized DAG-Based Consensus Algorithm,” DEXON Foundation, Taiwan, [Online]. Available: https://eprint.iacr.org/2018/1112.pdf.

[18] Department of Defense Trusted Computer System Evaluation Criteria, DoD, 1985. Available: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf.

Security Architectures in Digital Economy Systems

V. O. Piskovski, A. A. Grusho, M. I. Zabezhailo, A. V. Nikolaev, V. V. Senchilo, E. E. Timonina

***Abstract* — The article considers the task to protect information when an adversary uses methods of collecting valuable information on indirect signs in the information environment available to attackers. It is assumed that all personal data in the considered information space are anonymized. However, these measures are usually not enough. Using information links, it is possible to overcome the depersonalization of data, as well as to recover other valuable information about the activities of participants in the digital economy. To solve the problem of identifying intruders who are extracting information by indirect signs, it is necessary to have a means of registering subjects, organizations and individuals who have accessed certain data, possibly containing indirect signs of valuable information. Registering the facts of an access must be available on a public resource. If necessary, the registration tool should allow authorized users or a commission consisting of such users to obtain organization and person ids that have accessed the data. The purpose of such a log is to provide services for obtaining comprehensive and reliable information about whom, when and to what extent accessed personal or corporate data processed within the digital economy. It is proposed to use the distributed ledger architecture to solve the problem. This architecture allows you to store data on all calls to databases containing indirect information about valuable data. Protected analysis of the distributed ledger allows you to identify users who are trying to recover this information by indirect signs. At present, the technical and theoretical base is ready for the implementation of such solutions. The article lists the main components for such solutions.**

***Keywords* — information security, protection of valuable information from compromising on indirect signs, distributed register.**

REFERENCES

[1] BL and Big Data: Reviw TAdviser [Online] Available: https://www.tadviser.ru/index.php/BI.

[2] A. A. Grusho, N. A. Grusho, M. I. Zabezhailo, E. E. Timonina, "Protection of valuable information in public information space," *Communications of the ECMS. Proceedings of the 33th European Conference on Modelling and Simulation*, vol. 33, no. 1, pp. 451–455, 2019.

[3] A. A. Grusho, N. A. Grusho, M. I. Zabezhailo, E. E. Timonina. "Protection of valuable information in information technologies," Problems of information security. Computer systems, no. 2, pp. 22-26. 2018.

[4] Grusho, A., Ed. Primenko, and E. Timonina. *Theoretical bases of computer security*. Moscow: Academy. 2009.

[5] Su, Tzong-An and Gultekin Özsoyoglu. "Data Dependencies and Inference Control in Multilevel Relational Database Systems," in *1987 IEEE Symposium on Security and Privacy*, pp. 202-202, 1987.

[6] C. Stathakopoulou, C. Cachin, "Threshold Signatures for Blockchain Systems," Zurich: IBM Research, 2017. Available: https://pdfs.semanticscholar.org/2300/3bfc73e8d2fde9a465f4054f55ad1f2e8113.pdf?_ga=2.94560920.504720217.1596215569-1669259798.1588171840.

[7] Leemon Baird, "The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance," 2016. Available: https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf.

[8] Merkle Tree. [Online]. Available: https://en.wikipedia.org/wiki/Merkle_tree.

[9] Georg Becker, "Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis," 2008. [Online]. Available: https://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/becker_1.pdf.

[10] Rajeev Sobti, G.Geetha, "Cryptographic Hash Functions: A Review", *International Journal of Computer Science Issues*, vol. 9, issue 2, no 2, pp. 461-479, 2012. Available: https://www.researchgate.net/publication/267422045_Cryptographic_Hash_Functions_A_Review.

[11] Anton Churyumov, "Byteball: A Decentralized System for Storage and Transfer of Value," [Online]. Available: https://obyte.org/Byteball.pdf.

[12] Bjorn Hauge," SWIFTNet, VisaNet and Blockchain: The Future of Clearing," 2018, [Online]. Available: https://medium.com/datadriveninvestor/swiftnet-visanet-and-blockchain-the-future-of-clearing-f42de3ced34c.

[13] VISA, [Online]. Available: https://usa.visa.com/partner-with-us/payment-technology/visa-b2b-connect.html.

[14] Dr. Leemon Baird, Mance Harmon, and Paul Madsen, "Hedera: A Public Hashgraph. Network & Governing Council. The trust layer of the internet," 2019. [Online]. Available: https://www.hedera.com/hh-whitepaper-v1.4-181017.pdf.

[15] Eric Harris-Braun, Nicolas Luck, Arthur Brock, "Holochain. Scalable agent-centric distributed computing," DRAFT (ALPHA 1) - 2/15/2018. [Online]. Available: https://whitepaperdatabase.com/wp-content/uploads/2018/08/holochain-HOT-whitepaper.pdf.

[16] Directed Acyclic Graphs (DAGs). [Online]. Available: https://ericsink.com/vcbe/html/directed_acyclic_graphs.html.

[17] Tai-Yuan Chen, Wei-Ning Huang, Po-Chun Kuo, Hao Chung and Tzu-Wei Chao, "A Highly Scalable, Decentralized DAG-Based Consensus Algorithm," DEXON Foundation, Taiwan, [Online]. Available: https://eprint.iacr.org/2018/1112.pdf.

[18] Department of Defense Trusted Computer System Evaluation Criteria, DoD, 1985. Available: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf.