A Cryptographic Escrow for Treaty Declarations and Step-by-Step Verification
Sebastien Philippe, Alexander Glaser, and Edward W. Felten
Science and Global Security, 2019*,* Volume 27, No. 1, pp. 3-14

КРИПТОГРАФИЧЕСКОЕ УСЛОВНОЕ ДЕПОНИРОВАНИЕ ДЕКЛАРАЦИЙ ДОГОВОРА И ПОШАГОВАЯ ВЕРИФИКАЦИЯ

Себастьян Филиппе, Александер Глэзер, и Эдуард У. Фелтен

АННОТАЦИЯ

Верификация соглашений по контролю над вооружениями и разоружению требует от государств представления деклараций, включающих в себя информацию о секретных военных площадках и ресурсах. Однако, имеются важные случаи, в которых переговоры по таким соглашениям тормозятся из-за того, что стороны неохотно представляют любые такие данные из-за опасения преждевременной передачи информации, имеющей военное значение. Для решения данной проблемы мы предлагаем использовать криптографическое условное депонирование, которое позволяет государству в самом начале сделать полную декларацию площадок и ресурсов и согласиться с ее содержанием, но раскрывать его секретную информацию только поэтапно. В совокупности с режимом инспекции наше условное депонирование позволяет проводить пошаговую верификацию правильности и полноты первоначальной декларации таким образом, чтобы раскрытие информации и инспекции шли в ногу с параллельным дипломатическим и политическим процессами. Мы применяем этот подход к возможной денуклеаризации Северной Кореи. Однако, такой подход может быть применен к любому соглашению, требующему совместного использования засекреченной информации.

Себастьян Филиппе работает в Программе международной безопасности и Проекте по управлению атомом Центра Белфера научных и международных отношений Школы управления Джона Ф. Кеннеди Гарвардского университета, Кембридж, Массачусетс, США, и в Программе ядерного познания Центра международных исследований (CERI), Сьянс-По, Париж, Франция.

Александер Глэзер работает в Программе науки и всеобщей безопасности Принстонского университета, Принстон, Нью-Джерси, США.

Эдуард У. Фелтен работает в Центре политики информационных технологий Принстонского университета, Принстон, Нью-Джерси, США.

Почтовый адрес для корреспонденций: Sebastien Philippe, Belfer Center for Science and International Affairs, Harvard Kennedy School, 79 John F. Kennedy St, Mailbox 134, Cambridge, MA, 02138, USA

Адрес электронной почты: sebastien_philippe@hks.harvard.edu

ВВЕДЕНИЕ

Еще во время переговоров по ограничению стратегических вооружений между Соединенными Штатами и Советским Союзом договоры по контролю над ядерными вооружениями включали в себя мероприятия по обеспечению прозрачности и обмен информацией[1]. Однако, переговоры по глубоким сокращениям американского и российского ядерных арсеналов потребовали беспрецедентных раскрытий. В 1997 году в исследовании Национальной Академии Наук были предложены такие мероприятия по обеспечению прозрачности, как:

> «текущее местоположение, тип и статус всех ядерных взрывных устройств и история каждого изготовленного ядерного устройства, включая даты сборки и демонтажа или уничтожения во взрывных испытаниях; описание предприятий, на которых ядерные взрывные устройства были спроектированы, собраны, хранились, развертывались, обслуживались, и демонтировались, и которые производили или изготавливали ключевые компоненты оружия и ядерные материалы; и соответствующие эксплуатационные учетные документы таких предприятий»[2].

Такие раскрытия трудно реализовать, поскольку они могут предоставить противнику на ранней стадии существенную информация военного назначения. В исследовании 2005 года Комитет по международной безопасности и контролю над вооружениями Национальной Академии Наук сделал предположение, что криптография может помочь разрешить эту проблему[3].

Аналогичная проблема возникла сейчас в контексте переговоров между Соединенными Штатами и Корейской народной демократической республикой (КНДР) о создании на Корейском полуострове зоны, свободной от ядерного оружия, поскольку проблемы денуклеаризации во многом похожи на проблемы, связанные с глубокими сокращениями ядерных вооружений. Вполне вероятно, что от КНДР потребуют предоставить данные и раскрыть деятельность, относящуюся к ее программам ядерного оружия и баллистических ракет, а также подчиниться наблюдениям и инспекциям международного сообщества на месте[4].

Предшествующие планы верификации, предложенные Соединенными Штатами, требовали от КНДР представить существенные и подробные базовые декларации, включающие: текущее местоположение, тип и статус всех ядерных боеприпасов и связанных компонентов; описание предприятий, на которых ядерные материалы и боеприпасы были произведены, спроектированы, собраны, испытаны, хранились и развертывались; и данные о количестве и характеристиках декларированных ядерных материалов[5]. С точки зрения КНДР согласие на такие требования может оказаться слишком рискованным; это может потенциально предоставить Соединенным Штатам подробную карту ее военных и относящихся к ядерному оружию ресурсов на самой ранней стадии дипломатического процесса, что может стать важной угрозой безопасности, если переговоры сорвутся. Но учитывая сильную приверженность общественности США к верифицируемой денуклеаризации, трудно рассчитывать успешного дипломатического результата, если КНДР не предоставит полезную декларацию любого вида[6].

Здесь мы обращаемся к этой проблеме переговоров, представляя подход к декларациям, обеспечивающий безопасный для государства механизм передачи информации с последовательным раскрытием соответствующей секретной информации другому государству, и требующий от страны, делающей декларации, с самого начала связывать себя обязательством правильности и полноты своей первоначальной декларации, возможно даже, до того, как начнутся переговоры. Такая схема криптографического условного депонирования позволяет производить выдачу частичной информации для верификации на более поздних этапах, избежав рисков, связанных с одноразовой полной выдачей всех данных (смотрите рисунок 1). Это позволяет связать последовательный обмен данными с мероприятиями по укреплению доверия.

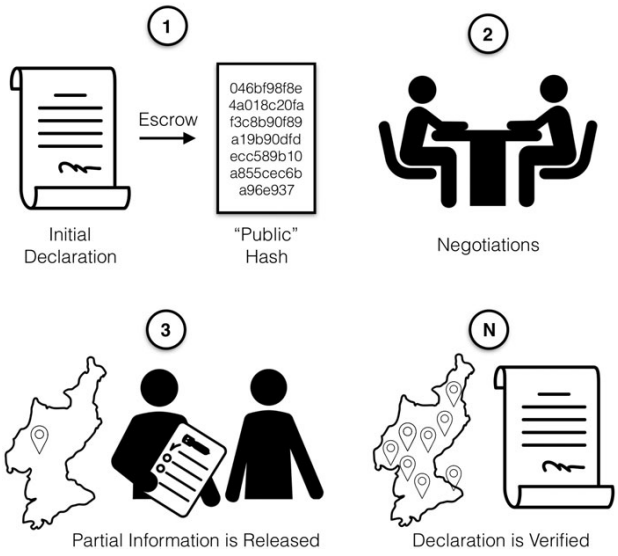

Рисунок 1. Использование криптографического условного депонирования в режиме инспекции. (1) Инспектируемая сторона готовит подробную первоначальную декларацию размещает ее в условном депонировании. Оглашается криптографическое обязательство по этой декларации. (2) Переговоры продолжаются. Условное депонирование построено таким образом, что оно позволяет раскрывать в определенный момент времени только частичную информацию. (3) Перед инспекцией на месте инспектирующей стороне раскрывается частичная информация о площадке (местоположение, статус, позиции). В конечном счете инспекции подтверждают правильность этой информации. (N) По мере продвижения переговоров информация раскрывается поэтапно, пока не будет раскрыта полная декларация. Только тогда инспектирующая сторона будет иметь полную картину ресурсов инспектируемой стороны.

Наше криптографическое условное депонирование использует криптографические примитивы в конкретных схемах передачи[7]. Такие схемы позволяют стороне обязаться представить конкретную часть информации, или величину, оставляя ее скрытой от других. Передающая сторона может раскрыть эту величину на более поздней стадии, гарантируя другим сторонам, что она не была изменена.

Хотя верификация денуклеаризации Северной Кореи – это особенно уместное применение нашего подхода, аналогичная схема условного депонирования может быть использована и в других международных соглашениях, включая обмен секретными декларациями как часть будущих российско-американских усилий по сокращению вооружений[3], или декларации засекреченной информации (например, идентификации и расположении источников загрязнения) в соглашениях по охране окружающей среды[8].

КОНСТРУКЦИЯ УСЛОВНОГО ДЕПОНИРОВАНИЯ

Базовой конструкцией нашего условного депонирования может быть криптографическое обязательство декларации в целом. Один из способов реализации схемы обязательства заключается в применении криптографических хеш-функций. Вообще говоря, хеш сообщения намного короче, чем само сообщение, а подлежащая криптографическая хеш-функция сконструирована таким способом, чтобы было невыполнимо определить действительное сообщение для заданного хеша (предполагая, что хешируемые величины были извлечены из случайного распределения с высокой энтропией), и чтобы было невыполнимо сконструировать два различных сообщения, которые обладали бы одним и тем же хешем (свойство, называемое устойчивостью к столкновению). В принципе, с помощью ошибкоустойчивых объединителей многих свойств могут быть объединены многие хеш-функции, так что каждое из необходимых криптографических свойств будет присуще комбинации, если оно присуще по крайней мере одной из объединяемых хеш-функций[9]. Это может быть использовано, например, для того, чтобы позволить каждой стороне в нашей схеме предложить хеш-функцию, которой он или она доверяют, и использовать комбинированную хеш-функцию, которая будет обладать желаемой безопасностью, если любая из выбранных сторонами хеш-функций будет безопасной.

Однако, простая передача полной декларации не предоставит никакой гибкости в том, как много информации, и какой, может быть передано в определенный момент времени. Для решения этого вопроса мы превратим наше условное депонирование в бинарное дерево Меркля (смотрите рисунок 2)[10]. Дерево строится следующим образом: каждый лист (или узел без потомков) может содержать любую строку (определенную как конечная последовательность символов), например, криптографическую передачу блока данных с информацией, относящейся к конкретной площадке, включая, в случае Северной Кореи, относящиеся к денуклеаризации позиции, хранящиеся на площадке. Любой узел, не являющийся листом, должен хранить величину Hash(L,R), когда в его левом потомке хранится L, а в правом – R. Корневой узел дерева представляет передачу декларации в целом, и он будет единственной частью информации, публикуемой в начале дипломатического процесса.

Кроме того, мы построили дерево, такое, что пара географических координат в стране соответствует уникальному листу в дереве. Для того, чтобы сделать это, мы наложили сетку на карту страны (смотрите рисунок 3). Для Северной Кореи сетка ограничена параллелями 37,5° с.ш. и 43,5° с.ш. и меридианами 124,0° в.д. и 131,0° в.д. Затем мы построили локальную систему координат (*i*,*j*) с началом координат в точке 43,5° с.ш. и 124,0° в.д. Количество точек в сетке зависит от выбранного разрешения по широте и долготе. Для разрешения в одну угловую минуту как по широте, так и по долготе (1,85 км по меридиану и 1,45 км по параллели), как это требуется в существующих соглашениях по контролю над вооружениями в отношении обмена информацией по координатам[11], количество точек будет равно 7·6·60·60 = 151200 точек. Каждая точка получает свой номер в соответствии с ее локальными координатами (*i*,*j*). Номера преобразуются в двоичные числа и сцепляются для получения соответствующего двоичного ключа x. Например, точка с координатами (7·60, 6·60) на карте с разрешением в одну минуту соответствует ключу x = 110100100101101000 длиной l = |x| = 18 бит.

Поскольку количество точек сетки не очень велико, мы выбрали упрощенную конструкцию, в которой каждой точке сетки соответствует свой листовой узел. В сценариях, в которых количество точек сетки может привести к непрактично большому размеру дерева, другие криптографические структуры данных могут предоставить необходимые свойства, не требуя от объявляющей стороны хранить данные для каждой пустой точки сетки[12].

В дереве глубиной *l*, каждый лист уникально доступен от корневого узла по пути, определяемому ключом *x* (смотрите рисунок 3), и содержит передачу данных о том, расположена ли площадка в данном местоположении, и любую другую соответствующую информацию о площадке, если таковая имеется. В случае Северной Кореи ожидается, что количество декларируемых площадок будет приблизительно равно 100 – 200[13], что намного меньше, чем количество листьев 2*l*. Эта конструкция позволяет извлекать информацию о любой точке сетки, или о любом подмножестве точек сетки, без передачи информации о любых других точках сетки.

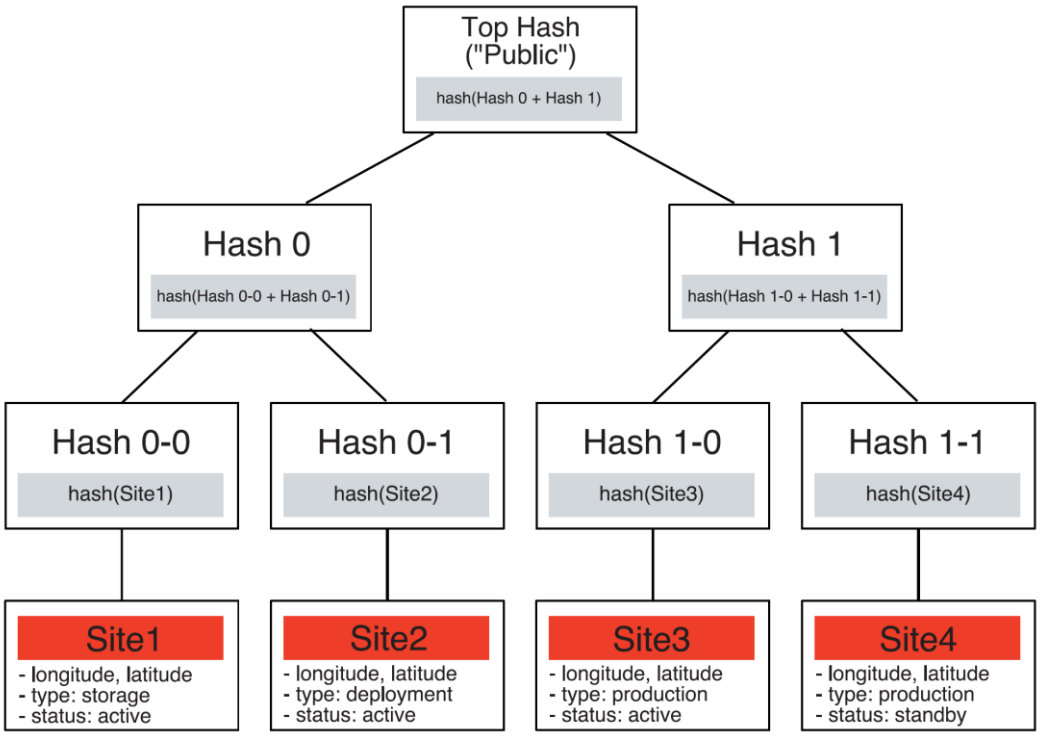

Рисунок 2. Декларация площадок с использованием структуры дерева Меркля. Каждый лист дерева содержит информацию по индивидуальным площадкам (отмечены как Site 1–4). Информация из каждого блока данных хешируется индивидуально, хеши верхних узлов «0» и «1» получаются хешированием сцепления двух нижних хешей до верхнего хеша, называемого также корнем дерева. Чтобы далее продемонстрировать, что информация по площадке 4 является частью декларации, сообщающей стороне нужно будет передать чистый текст по площадке 4, хеш площадки 4 (Hash 1-1), хеш 1-0, Hash 1 и верхний хеш. Этот процесс не раскрывает информацию о любых других площадках.

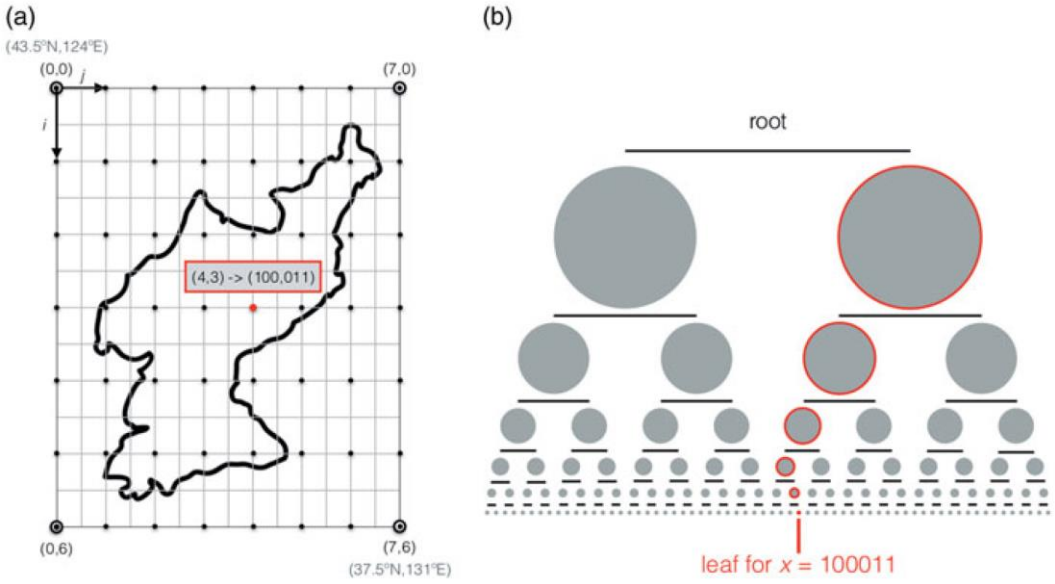

Рисунок 3. Отображение координат площадки на лист дерева Меркля. Локальные координаты (*i, j*) над КНДР (a) могут уникально с заданной точностью идентифицировать каждое местоположение в стране. После этого координаты (*i, j*) преобразуются в их двоичный эквивалент и сцепляются в строке x, соответствующей двоичному пути от корня до соответствующего листа в нашем дереве Меркля (b). Каждый лист в дереве либо сохраняет обязательство по информации о существующей площадке, либо остается пустым, если в этом местоположении нет никакой площадки.

ПОЭТАПНАЯ ВЕРИФИКАЦИЯ В СЦЕНАРИИ ЗАМОРАЖИВАНИЯ

На рисунке 4 представлено криптографическое обязательство (использующее хеш-функцию) по информации о гипотетической площадке хранения ядерного оружия, которое должно будет сохраняться в листе дерева, соответствующем местоположению площадки. Обязательство получается хешированием сообщения «m_0», содержащего различные части: случайное число, генерируемое обязующейся стороной, другое случайное число, предоставленное внешней стороной для гарантирования свежести информации (то есть того, что обязательство было произведено после того, как было генерировано случайное число внешней стороны)[14], информации, относящейся к включенной позиции, например, тип сооружения, координаты и статус, и, наконец, дополнительную информацию «m_1», которая представляет обязательства по дополнительным данным, которые могут быть исполнены на более поздней стадии, например, при инспекции соответствующей площадки.

Рисунок 4. Пример краткого изложения сообщения для площадки хранения. Информация скрывается на нескольких уровнях, которые могут быть раскрыты в различные моменты времени. Сообщение уровня 0 содержит случайное число, генерируемое владельцем, случайное число, предоставляемое инспектором для гарантирования свежести обязательства, данные чистого текста и хеш для сообщения уровня 1. Сообщение уровня 1 содержит дополнительные данные (в данном случае количество боеголовок, ракет, количества урана и плутония, и их изотопный состав), которые могут быть раскрыты на более поздней стадии, например, перед инспекцией. Краткие изложения сообщения (генерированные SHA3-256) предназначены только для иллюстрации.

В качестве предварительного этапа в верифицируемом процессе денуклеаризации, следующем фазированному подходу[15], КНДР могла бы согласиться на замораживание производства расщепляющихся материалов и компонентов для оружия, а также на мониторинг хранения существующего оружия. В такой структуре КНДР могла бы провести полное условное депонирование всех сведений о площадках производства, хранения и развертывания ядерного оружия, ракет, и связанных с ними компонентов. Затем она могла бы объявить наличие ресурсов на каждой площадке и согласиться не перемещать их с одной площадки на другую (маршруты перемещения между площадками могут отслеживаться со спутников). Для подтверждения правильности декларации КНДР могла бы пригласить Соединенные Штаты выполнить инспекции на месте и подтвердить, что ресурсы и информация, заявленная в условном депонировании, присутствуют, и верны. Во время таких инспекций подотчетные позиции могли бы быть помечены уникальными идентификаторами, а Соединенные Штаты могли бы стать более уверенными в том, что замораживание в самом деле действует, а остальная часть декларации, которая еще не была раскрыта, правильна[16].

Доверие с точки зрения Соединенных Штатов увеличилось бы, если площадки могли бы выбираться случайным образом[17], хотя КНДР может предпочесть раскрывать местоположение и запасы на каждой площадке в предпочитаемом ею порядке, например, начав с площадок, которые уже известны или считаются менее секретными. Поскольку каждая площадка может быть раскрыта без компрометации других объектов, темпы инспекции можно будет адаптировать к политическому процессу, что делает данный подход хорошо приспособленным к переговорному процессу «действие в ответ на действие», в котором обе стороны будут делать пошаговые уступки, двигаясь в сторону окончательного соглашения.

Комбинация свойств условного депонирования и возможность выполнения инспекций по запросу будет способствовать процессу установления полноты декларации. Если Соединенные Штаты полагают, что они обнаружили незаконную деятельность на необъявленной площадке, они могут предоставить Северной Корее координаты площадки, соответствующие специфическому ключу *x*. КНДР затем может доказать включение этой конкретной площадки в сусловное депонирование. Если площадка включена, то обе стороны могут подождать

и запланировать будущую инспекцию для подтверждения правильности декларации. Если площадка отсутствует в декларации, то надо будет провести специальную инспекцию для того, чтобы продемонстрировать, что на площадке не ведется никакой запрещенной деятельности. Учитывая риск обнаружения, в интересах КНДР будет с самого начала предоставить полную декларацию.

Помимо верификации сценариев замораживания, данная схема условного депонирования может быть адаптирована к принятию обязательств по позициям, материалам, и площадкам на периодической основе. Для каждого периода сторона, подготавливающая декларацию, будет криптографически подписывать обязательства таким образом, чтобы она не смогла отказаться от них впоследствии. Если такая подпись будет также покрывать хеш подписанного стороной обязательства за предыдущий период, то результатом станет криптографическая цепочка блоков, которая привязывает сторону к ее полной истории обязательств.

БЕЗОПАСНОСТЬ УСЛОВНОГО ДЕПОНИРОВАНИЯ

В целом, для жизнеспособности нашего подхода крайне важно, чтобы длина сообщения, содержание сообщения и реализация протокола обязательства были устойчивы ко всем соответствующим типам криптографических атак. При использовании хеш-функций важно помнить о потенциале атак на прообразы и атак столкновения хешей[18]. Атаки на прообразы стремятся определить сообщение, соответствующее данному хешу, построенному конкретной хеш-функцией. Это скомпрометирует секретность информации, помещенной в нашем условном депонировании. Однако, поиск столкновений и прообразов очень труден с вычислительной точки зрения, если использовался безопасный хеш. Например, если длина хеша равна n бит, где для современных хеш-функций n обычно равно 256 или 512, то криптоанализ методом прямого опробования потребует $2^{n/2}$ вычислений хеш-функции для поиска столкновений между двумя сообщениями, и 2^n вычислений для поиска прообразов и вторых прообразов. До сих пор успешных атак на прообразы для рекомендованных Национальным институтом стандартов и технологии США (NIST) хеш-функций не наблюдалось[19].

Однако, для старых и сейчас считающихся уязвимыми хеш-функций более типично обнаружение атак столкновения, которые могут создать проблемы для обязывающего свойства схемы передачи[20]. Последним практическим примером стало обнаружение первого столкновения для хеш-функции SHA-1 методом построения двух PDF документов с одним и тем же хешем[21]. Однако, открытие столкновения в SHA-1 ожидалось за много лет до того, как оно произошло. В нашем случае новые атаки столкновения могут повлиять на безопасность прошлых деклараций, если они позволят также проводить атаки вторичного прообраза. Эти риски могут быть ослаблены при использовании объединителей хеш-функций, позволяющих комбинировать несколько хеш-функций таким способом, что комбинация будет свободной от столкновений, если по крайней одна из составляющих хеш-функций будет свободна от стоклновений[22]. Если возникают сомнения в продолжающейся свободе от столкновений используемых хеш-функций, то обязательства могут быть регенерированы с помощью включения новой комбинации хеш-функций, обеспечивающих дополнительную защиту от столкновений.

ЗАКЛЮЧЕНИЕ

Дипломаты из Северной Кореи могут сесть за стол переговоров со своими коллегами из США с сообщением длиной в 256 или 512 бит на листочке бумаги. Используя разработанную в этой статье схему условного депонирования, такое простое сообщение может представить собой ключ к базе данных, содержащей каждый бит информации об их программах ядерного оружия и баллистических ракет. Такое действие может выполнить требование США о предоставлении всеобъемлющей информации о площадках и ресурсах. Оно не позволит также Соединенным Штатам уйти с переговоров с полученной информацией, создав потенциально неприемлемую угрозу безопасности Северной Кореи.

Мы показали, как совместить наше условное депонирование с режимом инспекции для верификации правильности и полноты декларации ядерных и других соответствующих площадок в пошаговом подходе. Хотя не вся информация будет заранее доступна инспекторам, доверие к достоверности декларации в целом будет возрастать с каждой успешной инспекцией. Наш подход также позволит инспектируемой стороне связать себя обязательством предоставить дополнительную информацию, документирующую конструкцию оружия, производственные записи, и перемещение ресурсов внутри оружейного комплекса.

Подход, представленный в этой статье, обладает потенциалом для разрешения давнишнего дипломатического тупика: Соединенные Штаты хотят получить точную и полную декларацию от КНДР, которая в свою очередь не хочет предоставлять перечень мишеней для превентивного военного нападения. Наше предложение разрешает это напряжение, позволяя КНДР взять обязательство по такой декларации, которая будет по-

степенно раскрываться по мере развития дипломатического процесса. В долгосрочном плане пример с Северной Кореей может служить важным прецедентом для применения современных криптографических методов для поддержки контроля над ядерным оружием и разоружения.

БЛАГОДАРНОСТЬ

Авторы благодарят Б. Барака, Р.Дж. Голдстоуна, Ф. фон Хиппеля, и З. Миана за их комментарии и отзывы.

ПРИМЕЧАНИЯ И ССЫЛКИ

1. J. Newhouse, *Cold dawn: The story of SALT* (Washington, DC: Pergamon, 1989).
2. National Academy of Sciences, *The Future of U.S. Nuclear Weapons Policy* (Washington, DC: National Academies Press, 1997).
3. Committee on International Security and Arms Control, *Monitoring Nuclear Weapons and Nuclear-Explosive Materials: An Assessment of Methods and Capabilities* (Washington, DC: National Academies Press, 2005).
4. A. Glaser and Z. Mian, “Denuclearizing North Korea: A verified, phased approach,” *Science,* 361 (2018): 981–983; R. S. Kemp, “North Korean disarmament: build technology and trust,” *Nature,* 558 (2018): 367–369; N. E. Busch and J. F. Pilat, *The Politics of Weapons Inspections: Assessing WMD Monitoring and Verification Regimes* (Stanford, CA: Stanford University Press, 2017).
5. International Panel on Fissile Materials, “U.S. proposal for verification of North Korea‘s denuclearization,” In Global Fissile Material Report 2009: A Path to Nuclear Disarmament (Princeton, IPFM, 2009), http://fissilematerials.org/library/gov08a.pdf .
6. V. P. Crawford, “A theory of disagreement in bargaining,” *Econometrica: Journal of the Econometric Society,* 50 (1982): 607–637; B. Levenotoglu and A. Tarar, “Prenegotiation commitment in domestic and international bargaining,” *American Political Science Review* 99 (2005): 419–433.
7. Перечень используемых в тексте криптографических терминов приведен в Приложении A. Математические определения большинства терминов можно найти в книге O. Goldreich, *Foundations of Cryptography* (New York, NY: Cambridge University Press, 2009).
8. S. Barrett, *Environment and Statecraft: The Strategy of Environmental Treaty-Making* (Oxford: Oxford University Press, 2003); National Research Council, *Verifying Greenhouse Gas Emissions: Methods to Support International Climate Agreements* (National Academies Press, 2010).
9. M. Fischlin, A. Lehmann, and K. Pietrzak, “Robust Multi-Property Combiners for Hash Functions,” *Journal of Cryptology,* 27 (2014): 397–428.
10. R. C. Merkle, “A Digital Signature Based on a Conventional Encryption Function,” *Lecture Notes in Computer Science,* 293 (1988): 369–378.
11. United States of America, Treaty between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms (2011).
12. S. Micali, M. Rabin, and J. Kilian, “Zero-Knowledge Sets,” In Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science, 11–14 October 2003, (Cambridge MA, 2003), 80–91.
13. M.J. Mazarr, G. Gentile, D. Madden, S. L. Pettyjohn, and Y. K. Crane, The Korean Peninsula: Three Dangerous Scenarios (RAND Corporation, 2018) https://www.rand. org/pubs/perspectives/PE262.html.
14. S. Haber and W. Stornetta, “How to Time-Stamp a Digital Document,” Advances in Cryptology-CRYPT0’90 Proceedings, Advances in Cryptology (1991): 437–455.
15. A. Glaser and Z. Mian, “Denuclearizing North Korea: A Verified, Phased Approach,” 981 (ссылка 4).
16. S. Fetter and T. Garwin, “Using tags to monitor numerical limits in arms control agreements,” In Blechman B.M. (ed.), *Technology and the Limitation of International Conflict*, (Washington, D.C.: Foreign Policy Institute, School of Advanced International Studies, Johns Hopkins University, 1989), 33–54.
17. D. M. Kilgour, “Site selection for on-site inspection in arms control,” *Contemporary Security Policy* 13 (1992): 439–462.
18. Устойчивость прообраза означает, что для любого вывода y хеш-функции h будет трудно вычислительно найти любой ввод x, который хешируется в тот же вывод, т.е. для заданного y трудно найти такое x, что h(x) = y. Устойчивость к столкновению (или устойчивость к второму прообразу) означает, что для любого ввода x трудно вычислительно найти любой другой ввод x’, который хешируется к тому же самому значению, то есть при заданном x трудно найти $x' \neq x$, такое, что h(x) = h(x’). Смотрите: P. Rogaway and T. Shrimpton, “Cryptographic hash-function basics: definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance,” In *Fast software encryption*, (Berlin/ Heidelberg: Springer,

2004), 371–388.
19. M. J. Dworkin, “SHA-3 standard: Permutation-based hash and extendable-output functions,” NIST, Federal Information Processing Standards, (NIST FIPS-202) (2015); Q. H. Dang, “Secure hash standard,” NIST, Federal Information Processing Standards (NIST FIPS-180-4) (2015).
20. X. Wang, and H. Yu, “How to break MD5 and other hash functions,” In EUROCRYPT Lecture Notes in Computer Science 3494 (2005): 19–35; S. Caskey, T. Draelos, R. Schroeppel, and K. Tolk, “Impacts of collisions within hashing algorithms and safeguards data,” In Proceedings of the 47th Institute of Nuclear Materials Management Annual Meeting, 16–20 July 2006 Nashville, TN (2006).
21. M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov, “The first collision for full SHA-1,” *Lecture Notes in Computer Science* 10401 (2017): 570–596.
22. Fischlin et al., “Robust multi-property combiners for hash functions,” 399 (ссылка 9).

ПРИЛОЖЕНИЕ А
СЛОВАРЬ КРИПТОГРАФИЧЕСКИХ ТЕРМИНОВ

В этом приложении приводится сводка определений важных криптографических концепций, определенных и обсуждаемых в основной статье. Определения представлены в порядке, подчеркивающем логические связи между ними.

Строка. Строка x – это конечная последовательность символов, принадлежащих к заданному алфавиту. Если алфавит является набором двоичных символов {0, 1}, то строка в алфавите {0, 1} будет конечной последовательностью битов, например, 01010 … 11010. Длина строки x, обозначаемая также как |x|, представляет количество символов в строке x. Например, если x = 010101, то |x| = 6.

Криптографический примитив. Криптографический примитив – это твердо установившийся алгоритм, который используется как базовый элемент для построения криптографических протоколов высокого уровня. Примеры криптографических протоколов включают односторонние функции, аутентификацию, шифрование и дешифрование, передачи и цифровые подписи.

Схема передачи. Схема передачи – это криптографический примитив, который позволяет стороне передать часть информации, или значение, сохраняя ее скрытой от других (также известно, как свойство скрытости). Передающая сторона может объявить скрытое значение на более поздней стадии, гарантируя другим сторонам, что оно не было изменено (также известно, как свойство *обязательности*).

Криптографическая хеш-функция. Криптографическая хеш-функция (часто для краткости называемая хеш-функцией) – это алгоритм, который отображает сообщение произвольной длины в строку фиксированной длины, называемую также *хешем* или *кратким изложением* сообщения. Хеш-функции детерминистичны: каждому сообщению всегда соответствует один и тот же хеш. Однако, малое изменение в сообщении приводит к большим изменениям получающегося хеша (свойство, известное как *лавинный эффект*). Хеш-функции должны легко рассчитываться – для любого сообщения m должно быть легко рассчитать x = H(m); но их должно быть исключительно трудно обратить – для заданного x поиск сообщения m такого, что H(m) = x, должен быть практически невыполнимым (свойство, известное как *необратимость*). Хеш-функции должны также быть также *устойчивыми к столкновению* – для любого ввода m должно быть трудно вычислить любой ввод m’, который приведет к тому же самому значению хеша, то есть при заданном m найти m’ ≠ m такое, что H(m) = H(m’). Благодаря их свойствам, хеш-функции могут быть использованы для реализации схем передачи.

Деревья. В компьютерных науках дерево – это тип данных, который представляет иерархическую древовидную структуру с *корневым* узлом, связанным с несколькими уровнями дочерних узлов, таких, что ни у одного дочернего узла не может быть больше одного родительского узла (смотрите рисунок A1). Структура связей должна быть ациклической, то есть такой, чтобы ни один из узлов не был родителем, или прародителем, или любым другим предком самого себя. Каждый узел в дереве может быть представлен как структура данных, состоящая из значения вместе с перечнем указателей на дочерние узлы. Дерево называют бинарным, если у каждого узла будет либо два потомка, либо ни одного.

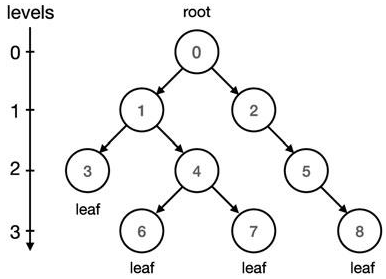

Рисунок А1. Пример древовидной структуры данных. Узел, обозначенный как 0, является корневым узлом дерева. Родителем узла 5 является узел 2. У узла 4 есть два потока, узлы 6 и 7. У узлов 3, 6, 7 и 8 потомков нет, и такие узлы называют листьями. Уровень узла соответствует его расстоянию от корня.

Хеш-дерево. Хеш-дерево (или дерево Меркля) – это дерево, в каждом листовом узле которого содержится хеш блока данных, и каждый не листовой узел которого имеет хеш, полученный хешированием конкатенации хешей дочерних узлов вплоть до верхнего хеша в корневом узле дерева (смотрите рисунок 2 основного текста статьи).