**Grammar Study**

|  |  |  |
| --- | --- | --- |
| **Grammatical feature** | **Context** | **Translation** |
| **ARTICLES** | | |
| *“A/An”- numerical meaning of oneness* | 1. Frequently, users on the web need to show that they are, for example, not **a robot**, old enough to access an age restricted video, or eligible to download an ebook from their local public library without being tracked. [1:1]  2. Here, both and could either be **a vector** of group elements or a vector of field elements. [3:8]  3. It also proposes **a solution** for higher-degree gates in the future work section but without security proof. [5:4] | 1. Часто пользователям в Интернете необходимо показать, что они, например, не **роботы**, достаточно взрослые, чтобы получить доступ к видео с возрастными ограничениями, или имеют право скачать электронную книгу из местной публичной библиотеки без слежки. [1:1]  2. Здесь A и B могут быть либо **вектором** элементов группы, либо вектором элементов поля. [3:8]  3. В разделе "Дальнейшее исследование" также предлагается **решение** для ворот более высоких степеней, но без доказательства безопасности. [5:4] |
| *“Zero article” - with uncountable nouns* | 1. Therefore, parties do not need to publish any **information** besides its public key. [3:10]  2. The drive is assumed to be ‘truthful’ in that it simply relays **information** about x and y as queried. [4:12]  3. An instantiation of zk-creds requires a publicly accessible bulletin board to distribute the credential list, as well as parties running our **software**. [1:24] | 1. Поэтому сторонам не нужно публиковать никакой **информации**, кроме своего открытого ключа. [3:10]  2. Предполагается, что диск является "правдивым", поскольку он просто передает **информацию** о x и y в соответствии с запросом. [4:12]  3. Для реализации zk-creds требуется общедоступная доска объявлений для распространения списка учетных данных, а также стороны, на которых работает наше **программное обеспечение**. [1:24] |
| *“A/An”- generic function* | 1. Scenario 2: **A cryptographer** walks into a bar. [1:27]  2. As a baseline, we can view the communication model discussed up until this point as **a simple direct access model**. [4:12]  3. **A special case** of this relation, used in a number of zero knowledge protocols, is known as the polynomial zero check. [4:15] | 1. Сценарий 2: **Криптограф** заходит в бар. [1:27]  2. В качестве базового варианта мы можем рассматривать модель коммуникации, обсуждавшуюся до этого момента, как **простую модель прямого доступа**. [4:12]  3. **Частный случай** этого отношения, используемый в ряде протоколов с нулевым знанием, известен как полиномиальная проверка нуля. [4:15] |
| *“Zero article” - generic function* | 1. We now build a system for in-person age verification coupled with **photographic verification**. [1:27]  2. Note that practical implementations of these protocols often involve careful considerations around **communication models** or cryptographic assumptions, which we elide here. [4:2]  3. There have been efforts to build accumulation **schemes** that overcome the limitations of fixed R1CS. [5:4] | 1. Теперь мы построим систему для проверки возраста при личной встрече в сочетании с **фотоверификацией**. [1:27]  2. Отметим, что практическая реализация этих протоколов часто требует тщательного рассмотрения **моделей связи** или криптографических предположений, которые мы здесь опускаем. [4:2]  3. Были предприняты попытки построить **схемы** накопления, которые преодолевают ограничения фиксированных R1CS. [5:4] |
| *“The”- generic function* | 1. Moreover, in **the event** the user has trustworthy secure hardware, they can self-issue the credential by attesting the hardware ran this notary check itself. [1:30]  2. We compress **the** prover **message** by committing to them in a homomorphic commitment scheme. [5:4]  3. We know that **the rate** of decay is no worse than that for parallel repetition of the MIP projection, and sometimes it equals that. [2:7] | 1. Более того, **если** у пользователя есть надежное защищенное оборудование, он может самостоятельно выдать учетную запись, заверив ее у нотариуса. [1:30]  2. Мы сжимаем **сообщение** проверяющего, принимая на себя обязательства по гомоморфной схеме. [5:4]  3. Мы знаем, что **скорость** распада не хуже, чем при параллельном повторении MIP-проекции, а иногда и равна ей. [2:7] |
| *“A/An”- first mention + “The” - second mention* | 1. Authority to issue **a credential** can be shown via zk-supporting-documentation that is itself the show of another credential. Moreover, because the proof in zk-supporting-documentation is general-purpose, the delegation process can constrain attributes in **the credential** being issued. [1:19]  2. Observe that, if **a user** has a valid Merkle authentication path (i.e., witness) attesting to their credential’s issuance at time , not all nodes in will usually need updating by time . Instead, **the user** only needs a summary of all Merkle tree nodes which have been added since time . [1:43]  3. The recursive circuit of this transformation is dominated by only scalar multiplications in the additive group of the commitment scheme for **a protocol** with prover messages and a degree d verifier. For R1CS, where and , this yields **the** same **protocol** and efficiency as Nova. [5:5] | 1. Полномочия на выдачу **удостоверения** могут быть продемонстрированы с помощью zk-supporting-documentation, которая сама является демонстрацией другой учетной записи. Более того, поскольку доказательство в zk-supporting-documentation является общим, процесс делегирования может ограничивать атрибуты в выдаваемом **удостоверении**. [1:19]  2. Обратите внимание, что если у **пользователя** есть действительный путь аутентификации Меркла (т.е. свидетель) , подтверждающий выдачу его мандата в момент времени , то обычно не все узлов в требуют обновления к моменту времени Вместо этого **пользователю** нужна только сводка всех узлов дерева Меркла, которые были добавлены с момента времени . [1:43].  3. Рекурсивная схема этого преобразования доминирует только над скалярными умножениями в аддитивной группе схемы обязательств для **протокола** с сообщениями проверяющего и верификатором степени . Для R1CS, где и , это дает тот же **протокол** и эффективность, что и в Nova. [5:5] |
| *“A/An”- when modified by a descriptive attribute* | 1. Concretely, identity assertions using zk-creds take less than 150ms in **a real-world** scenario of using a passport to anonymously access age-restricted videos. [1:1]  2. Finally, given the accumulation scheme, if the relation R is NP-complete, we can apply the compiler in [BCLMS21] to obtain **an efficient** IVC scheme with predicates expressed in R. [5:9]  3. Instead, our work shows that one can directly use parallel repetition for PCPs to reduce the soundness error to **an arbitrary** constant while preserving the query complexity . [2:7] | 1. В частности, подтверждение личности с помощью zk-creds занимает менее 150 мс в **реальном** сценарии использования паспорта для анонимного доступа к видео с возрастными ограничениями. [1:1]  2. Наконец, учитывая схему накопления, если отношение R является NP-полным, мы можем применить компилятор из [BCLMS21], чтобы получить **эффективную** схему IVC с предикатами, выраженными в R. [5:9].  3. Вместо этого в нашей работе показано, что можно напрямую использовать параллельное повторение для PCP, чтобы уменьшить погрешность обоснованности до **произвольной** константы при сохранении сложности запроса . [2:7]. |
| *“The”- when modified by a limiting attribute* | 1. In contrast to scanning the user’s driver’s license, this reveals **only** the minimal information necessary. [1:27] | 1. В отличие от сканирования водительского удостоверения пользователя, здесь можно получить **лишь** минимально необходимую информацию. [1:27] |
| *“The” - unique objects and notions* | 1. For this scenario, **the only issuer** is our passport-based issuer, and the access criteria being proved are age, expiry, and non-cloning. [1:26]  2. We consider an intermediate hybrid, where **the only difference** is in what is the aggregated signature and how the verification works. [3:36]  3. Fortunately, we observe that the syntactic mismatch of the messages sent by V and those sent by V′ is **the only issue** preventing us from concluding that MIP projection and PCP evaluation are inverses of each other. [2:31] | 1. Для этого сценария **единственным эмитентом** является наш эмитент на основе паспорта, а критериями доступа, которые необходимо подтвердить, являются возраст, срок действия и отсутствие клонирования. [1:26]  2. Мы рассматриваем промежуточный гибрид, в котором **разница лишь в том**, что является агрегированной подписью и как происходит проверка. [3:36]  3. К счастью, мы замечаем, что синтаксическое несоответствие сообщений, отправленных V и V′, — **единственная проблема**, мешающая нам сделать вывод, что MIP-проекция и PCP-оценка являются инверсиями друг друга. [2:31] |
| *“The” by reason of locality* | 1. This construction builds on **the results above**. [2:46]  2. We will focus almost universally on **the first part**: taking a large claim and reducing it to a much smaller one, such that it suffices only to verify the smaller claim, which, in turn, implies the original one with high probability. [4:13]  3. The relation statement can also add additional constraints on pc depending on **the applications**. [5:10] | 1. Эта конструкция опирается на **результаты, полученные выше**. [2:46]  2. Мы почти повсеместно сосредоточимся на **первой части**: берем большое утверждение и сводим его к гораздо меньшему, так что достаточно проверить только меньшее утверждение, которое, в свою очередь, с высокой вероятностью подразумевает исходное. [4:13]  3. Утверждение отношения может также добавлять дополнительные ограничения на pc в зависимости от **приложений**. [5:10] |
| *“The” when followed by an ordinal number* | 1. After **the first time**, the proof can be reused arbitrarily, until the user’s Merkle tree is updated by a new issuance. [1:29]  2. For example, the PCP for graph 3-coloring described above has soundness error less than 1 but its MIP projection has soundness error 1 (the first MIP prover always answers color 0 and **the second MIP prover** always answers color 1, regardless of the messages sent by the MIP verifier). [2:11]  3. **The first row** displays the native operations of the IVC prover. [5:27] | 1. После **первого раза** доказательство может быть использовано произвольно, пока дерево Меркле пользователя не будет обновлено новой выдачей. [1:29]  2. Например, PCP для 3-раскраски графа, описанная выше, имеет ошибку разумности меньше 1, но ее MIP-проекция имеет ошибку разумности 1 (первый MIP-доказатель всегда отвечает на цвет 0, а **второй MIP-доказатель** всегда отвечает на цвет 1, независимо от сообщений, отправленных MIP-верификатором). [2:11]  3. **В первой строке** отображаются собственные операции IVC-провера. [5:27] |
| *“Zero article” when the noun is followed by a cardinal number* | 1. This computation requires FFT (as noted in **Lemma 1**) and, hence, the aggregation time is . [3:36] | 1. Это вычисление требует БПФ (как отмечено в **Лемме 1**) и, следовательно, время агрегирования составляет . [3:36] |
| **ACTIVE VOICE** | | |
| *Present Simple* | 1. **We provide a toolchain** to convert a passport into an anonymous credential. [1:26]  2. **Parallel repetition refers to a set** of valuable techniques used to reduce soundness error of probabilistic proofs while saving on certain efficiency measures. [2:1]  3. **The scheme does not require a** trusted **setup** or pairings, and the prover does not need to compute any FFTs. [5:1] | 1. **Мы предоставляем инструментарий** для преобразования паспорта в анонимную учетную запись. [1:26]  2. **Параллельное повторение — это набор** ценных техник, используемых для уменьшения ошибки состоятельности вероятностных доказательств при сохранении определенных показателей эффективности. [2:1]  3. **Схема не требует доверенной установки** или сопряжений, и проверяющему не нужно вычислять никаких БПФ. [5:1] |
| *Present Continuous* | 1. However, in the current application, since **we are delegating** computation of a zkSNARK, we require the server’s output to be a publicly verifiable zkSNARK. [3:5]  2. In reality, there are multiple trust sources for a given identity attribute, their credentials have distinctively different formats, and many, if not all, **issuers are unwilling to adopt** new protocols. [1:1] | 1. Однако в данном приложении, поскольку **мы делегируем** вычисление zkSNARK, мы требуем, чтобы выход сервера был публично верифицируемым zkSNARK. [3:5]  2. В реальности существует множество источников доверия для данного идентификационного атрибута, их учетные данные имеют различные форматы, и многие, если не все, эмитенты **не желают принимать** новые протоколы. [1:1] |
| *Present Perfect* | 1. Thesepractical **constructions have opened a floodgate** of new applications. [3:3]  2. **We have used the fact** that in this bound. [4:11]  3. **We have discussed** conceptually simple access control **criteria** such as “my credential is not expired,” or “I am of age,” perhaps with a cryptographically complex mechanism for clone resistance. [1:28] | 1. Эти практичные **конструкции открыли простор** для новых применений. [3:3]  2. **Мы использовали тот факт**, что в этой границе. [4:11]  3. **Мы обсудили** концептуально простые **критерии** контроля доступа, такие как "мой мандат не просрочен" или "я совершеннолетний", возможно, с криптографически сложным механизмом для защиты от клонов. [1:28] |
| *Present Perfect Continuous* |  |  |
| *Past Simple* | 1. Prior to this work, **there were no known** black-box feasibility **results** for any of these applications. [3:1]  2. Note that, in the above construction, **we did not make use** of the freedom that many parameters, such as the distances between different elements, could be arbitrarily chosen. [4:33] | 1. До этой работы **не было известно** ни одного **результата** по выполнимости "черного ящика" для любого из этих приложений. [3:1]  2. Обратите внимание, что в приведенной выше конструкции **мы не использовали** свободу выбора многих параметров, например расстояний между различными элементами. [4:33] |
| *Past Continuous* |  |  |
| *Past Perfect* |  |  |
| *Future Simple* | 1. In this paper, **we will take** the linear-algebraic standard for notation (versus, e.g., some standards in coding theory). [4:2]  2. **A common view will be to look** at one specific element of the resulting vector Ax. [4:3] | 1. В данной работе **мы будем использовать** линейно-алгебраический стандарт обозначений (в отличие, например, от некоторых стандартов в теории кодирования). [4:2]  2. **Обычно рассматривается** один конкретный элемент результирующего вектора Ax. [4:3] |
| *Future Perfect* |  |  |
| **PASSIVE VOICE** | | |
| *Passive Voice (Present Simple)* | 1. Our polynomial commitment **is based on** the standard FRI-based polynomial commitment scheme. [3:4] | 1. Наше полиномиальное обязательство **основано на** стандартной схеме полиномиального обязательства на основе FRI. [3:4] |
| *Passive Voice (Present Continuous)* | 1. At a high level, this polynomial IOP performs the following operations on the extended witness (let R be the relation for which the proof **is being generated**). [3:28] | 1. На высоком уровне этот полиномиальный IOP выполняет следующие операции над расширенным свидетелем (пусть R - отношение, для которого **генерируется доказательство**). [3:28] |
| *Passive Voice (Present Perfect)* | 1. **These have been run** with hundreds of users and used to secure billions of dollars in cryptocurrency. [1:19]  2. Parallel **repetition has been studied** for interactive proofs (IPs) and multi-prover interactive proofs (MIPs). [2:1]  3. The **problem** of verifying privately delegated computation **has been studied** in prior works. [3:8] | 1. **Они работают** с сотнями пользователей и используются для защиты миллиардов долларов в криптовалюте. [1:19]  2. Параллельное **повторение было изучено** для интерактивных доказательств (IPs) и многопроверочных интерактивных доказательств (MIPs). [2:1]  3. **Проблема** проверки частного делегирования **вычислений изучалась** в предыдущих работах. [3:8] |
| *Passive Voice (Past Simple)* | 1. Michael Rosenberg’s work **was supported** by the National Defense and Engineering Graduate (NDSEG) Fellowship. [1:33]  2. Anonymous credentials **were developed** to address these concerns. [1:1]  3. Finally, we remark that before this work, the only black-box **construction** of a weighted threshold signature without setup **was proposed** by Micali et al. [3:7] | 1. Работа Майкла Розенберга **была поддержана** стипендией National Defense and Engineering Graduate (NDSEG). [1:33]  2. Для решения этих проблем **были разработаны** анонимные учетные данные. [1:1]  3. Наконец, отметим, что до этой работы единственная **конструкция** "черного ящика" взвешенной пороговой подписи без настройки **была предложена** Микали и др. [3:7] |
| *Passive Voice (Past Perfect)* |  |  |
| *Passive Voice (Future Simple)* | 1. In particular, users can (eventually) rely solely on broadcasted frontier nodes to update their authentication path , the Merkle forest scales effectively as the number of credentials grows, and **every user will be required** to update their credentials’ proofs of membership less often compared to a naïve Merkle tree construction of comparable capacity. [1:46] | 1. В частности, пользователи могут (в конечном счете) полагаться только на широковещательные пограничные узлы для обновления пути аутентификации , лес Меркля эффективно масштабируется с ростом числа учетных данных, и **каждому пользователю потребуется** обновлять доказательства принадлежности своих учетных данных реже по сравнению с наивной конструкцией дерева Меркля сопоставимой емкости. [1:46] |
| **VERBALS** | | |
| *Infinitive as a Subject or Attribute* | 1. We can use the rotation operation **to create** equivalence classes for verifier randomness, each class of size . [2:43] | 1. Мы можем использовать операцию вращения **для создания** классов эквивалентности для случайности верификатора, каждый класс размером . [2:43] |
| *Infinitive as a Predicate* | 1. A common view will be **to look** at one specific element of the resulting vector Ax. [4:3] | 1. Обычно **рассматривается** один конкретный элемент результирующего вектора Ax. [4:3] |
| *Infinitive as an Adverbial Modifier* | 1. However, **to ensure** the privacy of the secret witness employed in the generation of zkSNARK, **it is** highly **desirable** or, in many cases, necessary that this delegation remains privacy-preserving. [3:15] | 1. Однако для **обеспечения** конфиденциальности секретного свидетеля, используемого при генерации zkSNARK, крайне **желательно** или, во многих случаях, необходимо, чтобы это делегирование сохраняло конфиденциальность. [3:15] |
| *Complex Object with Infinitive* | 1. If n is large (say ) and , yet **we wish the probability** of failure **to be** no more than 2−100 then, repeating the experiment times suffices. [4:11] | 1. Если n велико (скажем, ) и , а мы **хотим, чтобы вероятность** неудачи непревышала 2–100, то достаточно повторить эксперимент раз. [4:11] |
| *Complex Subject with Infinitive* | 1. Clearly, this requires the verifier **to run** in time linear in . [3:11]  2. Indeed, we did not optimize for any constants at all, and, using the bounds presented here, the proof system would be **unlikely to be useful** for practical applications. [4:33] | 1. Очевидно, что это требует, чтобы верификатор **работал** за время, линейное по . [3:11].  2. Действительно, мы не оптимизировали ни для каких констант, и, используя представленные здесь ограничения, система доказательств **вряд ли будет полезна** для практических приложений. [4:33] |
| *Gerund as a Subject* | 1. Given issued credentials via passports, **building** a privacy-preserving age verification scheme with zk-creds **is straightforward** and requires no new cryptography: website developers need simply define the issuers they will accept and construct the access criteria they need using gadget. [1:26]  2. **Computing** this proof **takes** less than 2 seconds. [1:24] | 1. Учитывая выданные учетные данные через паспорта, **построение** схемы проверки возраста с сохранением конфиденциальности с помощью zk-creds **является простым** и не требует новой криптографии: разработчикам сайтов нужно просто определить эмитентов, которых они будут принимать, и создать необходимые критерии доступа с помощью гаджета. [1:26]  2. **Вычисление** этого доказательства **занимает** менее 2 секунд. [1:24] |
| *Gerund as an Adverbial Modifier* | 1. We associate to any given CSP a corresponding “canonical” PCP: the PCP string is the assignment to the variables of the CSP, and the PCP verifier samples a random constraint of the CSP and checks if it is satisfied (**by reading** from the PCP string the variables involved in that constraint). [2:5] | 1. Мы связываем с любым заданным CSP соответствующий “канонический” PCP: строка PCP — это назначение переменных CSP, а PCP-верификатор выбирает случайное ограничение CSP и проверяет его выполнение (**считывая** из строки PCP переменные, участвующие в этом ограничении). [2:5] |
| *Gerund as an Object (after preposition)* | 1. Finally, an issuer is able to revoke a credential if need be **by** simply **removing** it from the list. [1:14]  2. At a high level, we may view the above check as: we begin **by wishing to check** that some vector is -close to a subspace (of whatever dimension) embedded in . [4:32] | 1. Наконец, при необходимости эмитент может отозвать учетную запись, просто **удалив** ее из списка. [1:14]  2. На высоком уровне мы можем рассматривать описанную выше проверку следующим образом: мы начинаем **с желания проверить**, что некоторый вектор -близок к подпространству (любой размерности), вложенному в . [4:32] |
| *Gerund after Verbs (avoid, be worth, consider, finish, involve, allow, enable etc.)* | 1. Because zk-creds supports general purpose zero-knowledge proofs, geocoding restrictions are made more feasible with Groth16 gadgets: even if the Groth16 proof for the gadget is expensive, the resident or an outsourced prover **avoids recomputing** it every show. [1:29] | 1. Поскольку zk-creds поддерживает доказательства нулевого знания общего назначения, ограничения на геокодирование становятся более выполнимыми с помощью гаджетов Groth16: даже если доказательство Groth16 для гаджета дорого, резидентный или аутсорсинговый доказатель **избегает** его **повторного вычисления** при каждом показе. [1:29] |
| *Gerundial Complex* | 1. The benefit to this kind of customization is twofold: users can precompute and cache standalone gadget proofs separately from other access criteria proofs, and verifiers are freed **from having to define** custom circuits and generate the CRSs. [1:17] | 1. Выгода от такой настройки двойная: пользователи могут предварительно вычислять и кэшировать доказательства автономных гаджетов отдельно от других доказательств критериев доступа, а верификаторы освобождаются от **необходимости определять** пользовательские схемы и генерировать CRS. [1:17] |
| *Participle as an Attribute* | 1. We will use some of the checks presented above to present a protocol that successively reduces checking that some (potentially very large) vector is close to a subspace, to checking that an **appropriately-chosen** smaller vector is close to a vector subspace. [4:27]  2. The parameters **presented** above are relatively abstract. [4:33]  3. One particular example we will use constantly is the **vector space consisting of the evaluations** of a polynomial of small degree. [4:4] | 1. Мы используем некоторые из представленных выше проверок, чтобы представить протокол, который последовательно сводит проверку того, что некоторый (потенциально очень большой) вектор близок к подпространству, к проверке того, что **соответствующим образом выбранный** меньший вектор близок к векторному подпространству. [4:27]  2. **Представленные** выше параметры являются относительно абстрактными. [4:33]  3. Один конкретный пример, который мы будем постоянно использовать, это **векторное пространство, состоящее из значений** многочлена малой степени. [4:4] |
| *Participle as an Adverbial Modifier* | 1. Every issuer has some issuance criteria ι that the requester must meet **in order to have their cred issued**, e.g., that the birth date in cred matches a signed digital passport. [1:12] | 1. Каждый эмитент имеет некоторые критерии выдачи ι, которым должено соответствовать запрашивающее лицо, **чтобы получить своё удостоверение**: например, чтобы дата рождения в удостоверении соответствовала подписанному цифровому паспорту. [1:12] |
| *Absolute Participial Construction* | 1. However, in our current application, since the computation **being delegated to the server** is the generation of a zkSNARK, the resulting zkSNARK must, therefore, be publicly verifiable. [3:16] | 1. Однако в нашем текущем приложении, поскольку вычисления, **делегируемые серверу**, заключаются в генерации zkSNARK, результирующий zkSNARK, следовательно, должен быть публично верифицируемым. [3:16] |
| *Complex Object with the Participle* |  |  |
| *Complex Subject with the Participle* |  |  |
| **MODAL VERBS** | | |
| *Can / could / be able to* | 1. Note that, in the above construction, we did not make use of the freedom that many parameters, such as the distances between different elements, **could be arbitrarily chosen**. [4:33]  2. The tracking and data exposure risks raised by such requirements **can be eliminated** with privacy-preserving cryptography: anonymous credentials allow a user to assert that they meet some access criteria, e.g., are over 18, without revealing anything else about themselves, linking their viewing habits to their identity, or even linking distinct video views together. [1:2] | 1. Заметим, что в приведенной конструкции мы не использовали **свободу выбора многих параметров**, таких как расстояния между различными элементами. [4:33]  2. Риски отслеживания и раскрытия данных, связанные с такими требованиями, **можно устранить** с помощью криптографии, сохраняющей конфиденциальность: анонимные учетные данные позволяют пользователю подтвердить, что он соответствует некоторым критериям доступа, например, старше 18 лет, не раскрывая при этом ничего другого о себе, не связывая свои привычки просмотра с личностью и даже не связывая разные просмотры видео вместе. [1:2] |
| *May / might* | 1. Therefore, parties **may sample** their key pairs independently, and no interactive/trusted setup is required. [3:16]  2.To understand succinct proofs, **we may contrast** them with ‘traditional’ computational proofs; i.e., providing a witness for a given statement. [4:1]  3. Traditional computational proofs **may be viewed** as a certificate that a certain computation was performed correctly. [4:1] | 1. Таким образом, стороны **могут** самостоятельно **подбирать** свои пары ключей, и интерактивная/доверительная настройка не требуется. [3:16]  2.Чтобы понять краткие доказательства, **мы можем противопоставить** их "традиционным" вычислительным доказательствам, т.е. предоставлению свидетеля для данного утверждения. [4:1]  3. Традиционные вычислительные доказательства **можно рассматривать** как свидетельство того, что определенное вычисление было выполнено правильно. [4:1] |
| *Must / have to* | 1. Moreover, these proofs **must often be generated** obliviously, i.e., without knowledge of the secret. [3:1] | 1. Более того, эти доказательства **часто приходится генерировать** в беспамятстве, то есть без знания секрета. [3:1] |
| *Should / ought to* | 1. The proof size **should be sublinear** in the witness size. [3:18] | 1. Размер доказательства **должен быть сублинейным** по отношению к размеру свидетеля. [3:18] |
| **CONDITIONALS** | | |
| *Zero Conditional* | 1. We remark that, **if we want** the above protocol to be publically verifiable, **then we** crucially **require** the underlying LHEncap scheme to be linearly-homomorphic w.r.t. randomness. [3:13]  2. As a special case, **if the** underlying **LHEncap is deterministic**, **the** above **construction** **is** always publicly **verifiable**. [3:13] | 1. Заметим, что **если мы хотим**, чтобы приведенный выше протокол был публично проверяемым, **то нам** крайне **необходимо**, чтобы лежащая в его основе схема LHEncap была линейно гомоморфной по отношению к случайности. [3:13]  2. Как частный случай, **если** лежащая в основе **схема** LHEncap **детерминирована**, **то** приведенная выше **конструкция** всегда **поддается** публичной **проверке**. [3:13] |
| *I Conditional* |  |  |
| *II Conditional* |  |  |
| *III Conditional* |  |  |

**References:**

1. Michael Rosenberg et al. (2022). zk-creds: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure. *Cryptology ePrint Archive*. URL: <https://eprint.iacr.org/2022/878.pdf>.
2. Alessandro Chiesa et al. (2023). On Parallel Repetition of PCPs. *Cryptology ePrint Archive*. URL: <https://eprint.iacr.org/2023/1714.pdf>.
3. Sanjam Garg et al. (2023). How to Prove Statements Obliviously? *Cryptology ePrint Archive*. URL: <https://eprint.iacr.org/2023/1609.pdf>.
4. Alex Evans. (2023). Succinct Proofs and Linear Algebra. *Cryptology ePrint Archive*. URL: <https://eprint.iacr.org/2023/1478.pdf>.
5. Benedikt Bunz. (2023). Protostar: Generic Efficient Accumulation/Folding for Special-sound Protocols. *Cryptology ePrint Archive*. URL: <https://eprint.iacr.org/2023/620.pdf>.