Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н. Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н. Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления» (ИУ)
КАФЕДРА «Информационная безопасность» (ИУ8)

Выводы об оценке сложности протоколов безопасности на основе возведения в степень по схеме Диффи–Хеллмана и коммутируемого шифрования с открытым ключом

по дисциплине «Криптографические методы защиты информации»

Студент ИУ8-104 (Группа) Мильченко И. Д. (И. О. Фамилия) _____ (Подпись, дата)

Преподаватель Жуков А. Е. (И. О. Фамилия) _____ (Подпись, дата)

Оценка: _____

Москва, 2025 г.

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

Создание систем защищённого общения в открытых средах, таких как Интернет, представляет собой сложную задачу, существенно зависящую от используемых криптографических протоколов. Вместе с тем, на подобные системы можно осуществлять серьёзные атаки, эксплуатируя лишь внутренние уязвимости самих криптографических протоколов. Уязвимости криптографических протоколов легко пропустить на стадии проектирования, так как злоумышленник может контролировать сеть передачи данных и комбинировать сообщения, относящиеся к разным сеансам работы протокола. Кроме того, участники взаимодействия могут вести себя недобросовестно. Необходимость строгого формального анализа и наличия надёжных инструментов для анализа криптографических протоколов осознавалась уже давно. Так называемая модель Долева–Яо (Dolev–Yao), берущая начало из работы Долева и Яо [1], стала доминирующей формальной моделью анализа протоколов (см. обзор в [2]). Было предложено много процедур для автоматического анализа криптографических протоколов в рамках модели Долева–Яо [3], и на основе этих процедур разработаны многочисленные инструменты [4], которые успешно применялись для обнаружения уязвимостей в опубликованных протоколах [5].

Большинство методов и инструментов делают упрощающее предположение о том, что криптографические алгоритмы являются совершенными (предположение о совершенной криптографии). Иначе говоря, предполагается, что для извлечения открытого текста из зашифрованного сообщения необходим именно ключ шифрования; без него никакая информация об открытом тексте не может быть извлечена. Также предполагается, что зашифрованное сообщение может быть создано только при наличии соответствующего ключа и открытого текста. Однако такая простая модель становится недостаточной при анализе многочисленных протоколов, в которых используются операторы с алгебраическими свойствами, такие как исключающее ИЛИ (XOR) и модульное экспоненцирование. Причина этого двояка: во-первых, без учёта алгебраических свойств оператора протоколы могут не достигать целей безопасности даже без присутствия злоумышленника (в [6] приводится много таких примеров). Например, базовый протокол Диффи–Хеллмана явно использует коммутативность операции возведения в степень: $(g^a)^b = (g^b)^a$. Во-вторых, многие атаки основаны на эксплуатации именно алгебраических свойств операторов и поэтому не мо-

гут быть выявлены в рамках модели совершенной криптографии. Например, для рекурсивного протокола аутентификации Булла и Отвея [7] была доказана безопасность в предположении совершенных криптографических функций [8], однако он был впоследствии признан небезопасным при реализации на основе оператора XOR из-за его нильпотентности [9]. В разделе 6 приводится ещё один пример — протокол A-GDH.2 (см. [6]). Таким образом, при анализе современных криптографических протоколов важно учитывать алгебраические свойства операторов, таких как XOR, экспоненцирование Диффи–Хеллмана и RSA-шифрование.

Вклад данной работы. В этой работе мы показываем, что задача незащищённости протоколов, использующих экспоненцирование Диффи–Хеллмана с произвольными произведениями в показателях, является NP-полной при анализе в ограниченном числе сеансов. Мы демонстрируем, что наши модель протокола и модель злоумышленника достаточно выразительны, чтобы воспроизвести атаки, впервые описанные Pereira & Quisquater на примере протокола A-GDH.2 [10]. Аналогичный результат NP-полноты мы получаем и для протоколов с коммутирующим шифрованием с открытым ключом (например, RSA с общим модулем). В качестве следствия наших доказательств получаем, что задача вывода сообщения (derivation problem), то есть проверка возможности злоумышленника вывести заданное сообщение из конечного набора известных ему сообщений, решается за детерминированное полиномиальное время как для экспоненцирования Диффи–Хеллмана, так и для коммутирующего шифрования.

Наши доказательства NP-полноты строятся в два этапа. Сначала мы расширяем стандартную модель злоумышленника Долева–Яо с помощью обобщённых «правил-оракулов» и показываем, что общая задача незащищённости при таком расширении является NP-полной. Затем мы конкретизируем эти правила для экспоненцирования Диффи–Хеллмана и коммутирующего шифрования и показываем, что задачи вывода и анализа безопасности протокола решаются за детерминированное и недетерминированное полиномиальное время соответственно.

Связанные работы. Первые исследования, рассматривающие алгебраические свойства операторов, включая их в модель Долева–Яо, были выполнены Chevalier et al. [11] и Comon-Lundh & Shmatikov [12], где модель была расширена оператором XOR и его свойствами. Для экспоненцирования Диффи–Хеллмана

и коммутирующего шифрования, как показано здесь, ситуация сложнее: в отличие от XOR, мы не имеем нильпотентного свойства и должны учитывать число вхождений элементов в произведении, что требует решения уравнений над целыми числами.

Meadows & Narendran [13] разработали алгоритмы унификации для свойств криптографических систем на основе схемы Диффи–Хеллмана. Эти результаты полезны, но не решают более общую проблему незащищённости (см. также [14]).

Pereira & Quisquater [15] предложили систематический метод анализа семейств протоколов, расширяющих схему обмена ключами Диффи–Хеллмана до группового контекста. Хотя они обнаружили интересные атаки, основанные на алгебраических свойствах экспоненцирования, они не исследуют вопросы разрешимости и сложности.

Goubault-Larrecq et al. [16] создали систему верификации протоколов с модульным экспоненциацированием на фиксированном генераторе g. Их метод основан на аппроксимациях и включает правило вывода, позволяющее злоумышленнику получить $g^{a \cdot b}$ из g^a и b, но не учитывает обратимые операции и потому упускает реалистичные атаки.

Boreale & Buscemi [17] рассмотрели схожую задачу, но ввели априорную границу на число множителей в произведениях, тогда как в нашей работе число множителей неограниченно; кроме того, они не дают результатов о сложности.

Millen & Shmatikov [18] исследовали абелевы группы и применяли их к экспоненцирования Диффи–Хеллмана, но не предложили алгоритма решения и предполагали фиксированную основу в показателях. Shmatikov [19], опираясь на результаты Chevalier et al. [20], предложил процедуру для поиска атак в варианте нашей модели, но также не дал оценок сложности. В отличие от нашего подхода, в его модели множители могли находиться вне показателей, а сами множители не начинаться с операции экспоненцирования, что является дополнительным ограничением.

Структура работы. В разделе 2 мы вводим нашу модель протокола и злоумышленника, включая упомянутые правила-оракулы. В разделе 3 доказывается NP-полнота общей задачи незащищённости. В разделах 4 и 5 эти правила конкретизируются для экспоненцирования Диффи–Хеллмана и коммутирующего шифрования, и демонстрируется, что задачи вывода и анализа безопасности решаются за детерминированное и недетерминированное полиномиальное

время соответственно. В разделе 6 формализуется протокол A-GDH.2 и приводится атака, впервые описанная Pereira & Quisquater [10]. В разделе 7 наш метод применяется к протоколам с коммутирующим шифрованием. Заключение содержится в разделе 8. Некоторые подробности доказательств вынесены в приложение.

2 Протокол и модель злоумышленника

Модель протокола и злоумышленника, которую мы описываем далее, расширяет стандартные модели для (автоматического) анализа протоколов безопасности [3] в двух отношениях. Во-первых, сообщения могут строиться с помощью оператора $Exp(\cdot,\cdot)$, означающего экспоненцирование, и оператора произведения "$\cdot$". Во-вторых, помимо стандартных правил перезаписи модели Долева–Яо, злоумышленник снабжён дополнительными «правилами-оракулами», которые будут конкретизированы правилами экспоненцирования термов. В дальнейшем мы приведём формальное определение нашей модели, задав терминологию для термов, сообщений, протоколов, злоумышленника и атак.

2.1 Термы и сообщения

Множество термов *term* определяется следующей грамматикой:

$$\begin{aligned} term ::= \;& \mathcal{A} \mid \mathcal{V} \mid (term, term) \mid \{term\}^s_{k_{term}} \\ & \mid \{term\}^p_k \mid Exp(term, product) \\ product ::= \;& term^{\mathbb{Z}} \mid term^{\mathbb{Z}} \cdot product \end{aligned}$$

где $\mathcal{A}$ — конечное множество констант (атомарных сообщений), включающее имена субъектов, случайные значения, ключи, и специальные константы 1 и "секрет". Множество $\mathcal{K} \subseteq \mathcal{A}$ содержит все открытые и закрытые ключи. $\mathcal{V}$ — конечное множество переменных, $\mathbb{Z}$ — множество целых чисел, используется для показателей в произведениях. Предполагается, что существует биекция $.^{-1} : \mathcal{K} \to \mathcal{K}$, сопоставляющая каждому открытому (закрытому) ключу k соответствующий закрытый (открытый) ключ k^{-1}.

Бинарный символ $\langle\cdot,\cdot\rangle$ обозначает объединение в пару, символ $\{\cdot\}^s$ используется для симметричного шифрования, а символ $\{\cdot\}^p$ — для шифрования с открытым ключом. Заметим, что симметричный ключ может быть произвольным термом, в то время как для шифрования с открытым ключом допускаются только атомарные ключи из $\mathcal{K}$.

Оператор произведения "$\cdot$" моделирует умножение в абелевой группе. Например, произведение $a^2 \cdot b^3 \cdot c^{-2}$ представляет элемент этой группы, где $a^2 = a \cdot a$, $b^3 = b \cdot b \cdot b$, а $c^{-2} = c^{-1} \cdot c^{-1}$, причём c^{-1} — обратный к c. В протоколе A-GDH.2, к примеру, в качестве абелевой группы используется под-

группа G порядка q мультипликативной группы $\mathbb{Z}_p^*$, где p и q — простые числа. Термы и произведения рассматриваются с учётом коммутативности и ассоциативности оператора $\cdot$, а также с учётом тождества $t^1 = t$. Например, термы $d^1 \cdot c^{-2} \cdot (b^3 \cdot a^2)$ и $a^2 \cdot b^3 \cdot c^{-2} \cdot d$ считаются представлениями одного и того же произведения. Также, если мы пишем $t_1^{z_1} \cdots t_n^{z_n}$, то всегда предполагается, что символ t_i не является произведением. Этого можно достичь, расставив скобки соответствующим образом. Мы используем обозначение $t_1^{z_1} \cdots t_n^{z_n}$ для обозначения произведения, где z_i — некоторые ненулевые целые числа. Оператор $Exp(\cdot, \cdot)$ означает возведение в степень. Например, $Exp(a, b^2 \cdot c^{-1}) = a^{b^2 \cdot c^{-1}}$.

Если $t, t_1, \ldots, t_n$ — термы и $n \geq 2$, то произведение вида t^z (при $z \neq 1$) или вида $t_1^{z_1} \cdots t_n^{z_n}$ называется *нестандартным термом* (non-standard term). Мы часто обозначаем терм или произведение как *терм*. Чтобы различать их, мы используем понятие *стандартного терма*, противопоставляя его нестандартному.

Переменные обозначаются $x, y, \ldots$, а сами термы — s, t, u, v. Конечные множества термов пишем $E, F, \ldots$ и их индексированные варианты. Для краткости будем записывать $E \cup F$ как $E, F,$ объединение$E \cup \{t\}$ как $E, t,$ и$E \setminus \{t\}$ как $E \setminus t$.

Для терма t и множества термов E через $\mathcal{V}(t)$ и $\mathcal{V}(E)$ обозначим соответственно множество переменных, встречающихся в t и в E.

Терм основания (также называемый сообщением) — это терм без переменных. Мы используем выражения *стандартные* и *нестандартные сообщения* так же, как мы используем стандартные и нестандартные термы. Подстановка σ — это отображение из $\mathcal{V}$ в множество стандартных термов основания. Применение σ к терму t (или множеству E) обозначается $t\sigma$ (соответственно $E\sigma$) и определяется обычным образом.

Скажем, что термы t и t' *совпадают с точностью до показателей произведения* (пишем $t \approx t'$), если они различаются только значениями степеней. Например:

$$\begin{aligned} \langle Exp(g, a^2),\ Exp(g, b^{-3} \cdot c) \rangle &\approx \langle Exp(g, a^0),\ Exp(g, b^2 \cdot c^5) \rangle \\ &\not\approx \langle Exp(g, b^1),\ Exp(g, a^2 \cdot c^5) \rangle \end{aligned}$$

Отношение естественно расширяется на подстановки: $\sigma \approx \sigma'$ тогда и только тогда, когда $\sigma(x) \approx \sigma'(x)$ для любой переменной x.

Пусть u — стандартный терм, а v — произвольный терм. *Замена* $\delta = [u \mapsto v]$ отправляет любой терм t в терм $t\delta = t[u \leftarrow v]$, полученный заменой всех вхождений u на v.

Определение 2.1. Применение замены $\delta = [v \leftarrow\!\shortmid u]$ к терму t (обозначается $t\delta$) задаётся индукцией по структуре t:

- If $t = u$, $t\delta = v$.
- If $t \in \mathcal{A} \cup \mathcal{V},\ t \neq u$, $t\delta = t$.
- If $t = \langle t_1, t_2 \rangle$, $t\delta = \langle t_1\delta,\ t_2\delta \rangle$.
- If $t = \{t_1\}^s_k$, $t\delta = \{t_1\delta\}^s_{t_2\delta}$.
- If $t = \{t_1\}^p_k$, $t\delta = \{t_1\delta\}^p_{t_2\delta}$.
- If $t = Exp\big(t_0,\ t_1^{z_1} \cdots t_p^{z_p}\big)$, $t\delta = Exp\big(t_0\delta,\ (t_1\delta)^{z_1} \cdots (t_p\delta)^{z_p}\big)$.
- If $t = t_1^{z_1} \cdots t_p^{z_p}$, $t\delta = (t_1\delta)^{z_1} \cdots (t_p\delta)^{z_p}$.

Например, для $\delta = [Exp(g, a) \leftarrow\!\shortmid 1]$ имеем $Exp(g, a^2)\delta = Exp(g, a^2)$, и $Exp(g, a \cdot b)\delta = Exp(g, a \cdot b)$. По определению результат $t\delta$ единствен.

Подстановку σ можно сочетать с заменой δ: композиция $\sigma\delta$ даёт подстановку, определяемую правилом $x(\sigma\delta) = (x\sigma)\delta$ для всех $x \in \mathcal{V}$.

Множество всех подтермов $S(t)$ определяется так:

- Если $t \in \mathcal{A}$ or $t \in \mathcal{V}$, $S(t) = \{t\}$;
- Если $t = \langle u, v \rangle,\ \{u\}^s_v,$ or $\{u\}^p_v$, $S(t) = \{t\} \cup S(u) \cup S(v)$;
- Если $t = Exp\big(u, t_1^{z_1} \cdots t_p^{z_p}\big)$, $S(t) = \{t\} \cup S(u) \cup \bigcup_{i=1}^{p} S(t_i)$;
- Если $t = t_1^{z_1} \cdots t_p^{z_p}$, $S(t) = \{t\} \cup \bigcup_{i=1}^{p} S(t_i)$.

Здесь все t_i предполагаются стандартными термами.

Мы полагаем $S(E) = \bigcup_{t \in E} S(t)$. Заметим, что $Exp(a, b^2 \cdot c^1)$ и $b^2 \cdot c^1 \cdot d^1$ *не* являются подтермами терма $Exp(a, b^2 \cdot c^1 \cdot d^1)$.

Множество *расширенных подтермов* терма t определим как $S_{\text{ext}}(t) = S(t) \cup \{\, M \mid Exp(u, M) \in S(t)\}$. Иными словами, если в t встречается подтерм вида $Exp(u, M)$, то само произведение M также включается в $S_{\text{ext}}(t)$.

Множество факторов терма t, обозначаемое $\mathcal{F}(t)$, определяется рекурсивно:

– Если t является стандартным и не содержит $Exp(\cdot,\cdot)$, то $\mathcal{F}(t) = \{t\}$.
– Если $t = Exp(u, t_1^* \cdots t_p^*)$, то $\mathcal{F}(t) = \{u, t_1, \ldots, t_p\}$.
– Если $t = t_1^* \cdots t_p^*$, то $\mathcal{F}(t) = \{t_1, \ldots, t_p\}$.

Заметим, что $\mathcal{F}(t)$ содержит только стандартные термы. Например, при $a, b, c \in \mathcal{A}$ имеем $\mathcal{F}\big(a^2 \cdot b^1 \cdot c^{-1}\big) = \{a, b, c\}$.

Рассмотрим два способа измерения «размера» терма. В одном случае учитывается произведение в показателях, в другом — нет. В любом случае размер определяется по DAG-представлению терма: $|t| := \mathrm{Card}\big(S(t)\big)$ ($|t|_{\mathrm{ext}} := \mathrm{Card}\big(S_{\mathrm{ext}}(t)\big)$, то есть как количество (расширенных) подтермов t.

Замечание 2.2. Всегда выполняется неравенство $|t|_{\mathrm{ext}} \le 2\,|t|$.

Определения $|\cdot|$ и $|\cdot|_{\mathrm{ext}}$ не учитывают длину показателей. Чтобы измерить объём памяти, необходимый для их хранения, введём

$$\|t\|_{\exp} := \sum_{t_i^{z_i} \cdots t_n^{z_n} \in S(t)} |z_i| + \cdots + |z_n|,$$

где $|z_i|$ — число битов в двоичной записи целого z_i.

Полный размер терма определяется как

$$\|t\| := |t| + \|t\|_{\exp}.$$

Для множества термов E размер задаётся аналогично (заменой t на E). Для подстановки σ положим

$$|\sigma| := \sum_{x \in \mathcal{V}} |\,\sigma(x)|,$$

и аналогично, мы определим $\|\sigma\|_{\exp}$, $\|\sigma\|$. При помощи структурной индукции нетрудно показать:

Лемма 2.3. Пусть s — стандартный терм, t — терм, а x — переменная либо атомарное сообщение. Обозначим через δ замену $[s \leftarrow x]$. Тогда выполняется неравенство $|t\delta| \le |t|$.

Теперь сформулируем алгебраические свойства термов. Напомним, что все термы рассматриваются с точностью до коммутативности и ассоциативности оператора произведения, а также до тождества $t^1 = t$. Кроме того, мы пользуемся следующими равенствами:

$$t \cdot 1 = t \tag{1}$$
$$t^0 = 1 \tag{2}$$
$$1^z = 1 \tag{3}$$
$$t^z \cdot t^{z'} = t^{z+z'} \tag{4}$$
$$Exp(t, 1) = t \tag{5}$$
$$Exp\big(Exp(t, t'), t''\big) = Exp\big(t, t' \cdot t''\big) \tag{6}$$

Нормальные формы множеств термов и подстановок определяются аналогично. Терм t называется нормализованным, если $\ulcorner t \urcorner = t$. Нормализованные множества и подстановки вводятся тем же образом. Два терма t и t' считаются эквивалентными (modulo Exp и „$\cdot$“), если $\ulcorner t \urcorner = \ulcorner t' \urcorner$. Легко показать:

Лемма 2.4. Для любых термов t, t' и подстановки σ верны соотношения

(1) $S\big(\ulcorner t \urcorner\big) \subseteq S(t)$,
(2) $\big\|\ulcorner t \urcorner\big\|_{\exp} \leq \|t\|_{\exp}$,
(3) $\big\|\ulcorner t \urcorner\big\| \leq \|t\|$,
(4) $S(t\sigma) \subseteq S(t) \cup S\big(\mathcal{V}(t)\sigma\big)$,
(5) $\ulcorner t\sigma \urcorner = \ulcorner\ulcorner t \urcorner\sigma \urcorner = \ulcorner t\ulcorner\sigma\urcorner\urcorner = \ulcorner\ulcorner t\urcorner\ulcorner\sigma\urcorner\urcorner$.

2.2 Модель нарушителя

Наша модель злоумышленника соответствует модели злоумышленика Долева–Яо [Dolev & Yao, 1983]: злоумышленник полностью контролирует сеть и может выводить новые сообщения как из своего начального набора знаний, так и из перехваченных сообщений честных участников во время работы протокола. Для этого он способен составлять и разбирать термы, шифровать и расшифровывать данные при наличии соответствующего ключа, а также свободно

комбинировать эти операции. Классическая модель дополнена у нас особыми угадывающими правилами (*guess rules*), расширяющими возможности нарушителя по выводу сообщений; правила, удовлетворяющие дополнительным условиям (см. раздел 2.5), мы называем *оракульными правилами*.

Злоумышленник выводит новые сообщения из заданного (конечного) множества сообщений путём применения его правил. Правило злоумышленника (или t-правило) L имеет вид $S \longrightarrow t$, где S — конечное множество стандартных сообщений, а t — стандартное сообщение. Пусть E — конечное множество стандартных сообщений. Тогда L применимо к E тогда и только тогда, когда $S \subseteq E$. Определим *шаг по правилу* L как бинарное отношение $\to_L$ на множествах стандартных сообщений; в частности, $E \to_L E \cup \{t\}$ если $L\colon S \to t$ и $S \subseteq E$. Для семейства правил $\mathcal{L}$ (конечного или бесконечного) вводится объединённое отношение $\to_{\mathcal{L}} = \bigcup_{L\in\mathcal{L}} \to_L$, а его рефлексивное и транзитивное замыкание обозначается $\to^*_{\mathcal{L}}$.

Набор правил злоумышленника, рассматриваемых в данной работе, приведён в Таблице 1. В ней m, m' обозначают произвольные стандартные сообщения, $k \in \mathcal{K}$ — произвольный ключ, а E — конечное множество стандартных сообщений.

Таблица 1 – Правила злоумышленника

	Правила разложения	**Правила композиции**
Пара	$L_{p1}(\langle m, m'\rangle)\colon \langle m, m'\rangle \mapsto m$, $L_{p2}(\langle m, m'\rangle)\colon \langle m, m'\rangle \mapsto m'$	$L_c(\langle m, m'\rangle)\colon m, m' \mapsto \langle m, m'\rangle$
Асимметричное	$L_{ad}(\{m\}^p_K)\colon \{m\}^p_K,\ K^{-1} \mapsto m$	$L_{ec}(\{m\}^p_K)\colon m,\ K \mapsto \{m\}^p_K$
Симметричное	$L_{sd}(\{m\}^s_{m'})\colon \{m\}^s_{m'},\ m' \mapsto m$	$L_{sc}(\{m\}^s_{m'})\colon m,\ m' \mapsto \{m\}^s_{m'}$
Guess	$L_{od}(m)\colon E \mapsto m$, *где* m *— подтерм* E *и* E *нормализован*	$L_{oc}(m)\colon E \mapsto m$, *где* E, m *нормализованы и каждый настоящий подтерм* m *является подтермом* E

Отметим, что термин «правило злоумышленника» впредь будет применяться исключительно к правилам, перечисленным в Таблице 1. На данный момент под этим могут пониматься любые правила угадывания из таблицы, однако позднее (см. раздел 2.5) мы выделим специальные классы таких правил, называемые оракульными правилами.

Правила злоумышленника заданы, как в Таблице 1. Множества $L_{od}(m)$ и $L_{oc}(m)$ обозначают (конечные или бесконечные) совокупности угадывающих правил. Для единообразия мы рассматриваем $L_{p1}(\langle m, m' \rangle), \ldots, L_{sd}(\{m\}^s_{m'})$ и $L_c(\langle m, m' \rangle), \ldots, L_c(\{m\}^s_{m'})$ как отдельные синглтоны. Заметим, что даже при отсутствии угадывающих правил число правил разложения и композиции остаётся бесконечным, поскольку сообщений m, m' существует бесконечно много. Далее мы сгруппируем правила злоумышленника следующим образом. Во всех последующих формулах t пробегает по всем стандартным сообщениям.

Далее мы группируем правила злоумышленника по категориям. Во всех последующих формулах t пробегает по всем стандартным сообщениям.

— $L_d(t) := L_{p1}(t) \cup L_{p2}(t) \cup L_{ad}(t) \cup L_{sd}(t)$, если t не является парой, то $L_{p1}(t) = \emptyset$ (аналогично для остальных).
— $L_d := \bigcup_t L_d(t), \quad L_c := \bigcup_t L_c(t),$
— $L_{od} := \bigcup_t L_{od}(t), \quad L_{oc} := \bigcup_t L_{oc}(t),$
— $L_o(t) := L_{oc}(t) \cup L_{od}(t), \quad L_o := L_{oc} \cup L_{od},$
— $\mathcal{L}_d := \bigcup_t \mathcal{L}_d(t)$, где $\mathcal{L}_d(t)$ — множество всех t-правил разложения (левая колонка Таблицы 1);
— $\mathcal{L}_c := \bigcup_t \mathcal{L}_c(t)$, где $\mathcal{L}_c(t)$ — множество всех t-правил композиции (правая колонка Таблицы 1);
— $\mathcal{L} := \mathcal{L}_d \cup \mathcal{L}_c$.

Заметим, что $\mathcal{L}$ обозначает (бесконечный) набор всех правил злоумышленника, рассматриваемых здесь. Множество сообщений, которое злоумышленник может получить из конечного множества сообщений E, определяется так:

$$\mathit{forge}(E) := \{ E' \mid E \to^*_{\mathcal{L}} E' \}.$$

Из определения правил злоумышленника в Таблице 1 непосредственно следует:

Лемма 2.5. Пусть E — нормализованное множество сообщений. Тогда множество $\mathit{forge}(E)$ также является нормализованным.

Лемма означает, что если злоумышленник оперирует лишь нормализованными сообщениями, то он не может получить ничего иного, кроме нормализованных сообщений. Модель злоумышленника выстраивается так, чтобы он не умел различать эквивалентные сообщения. В дальнейшем мы всегда предполагаем, что знания злоумышленника составляют именно множество нормализованных сообщений, каждое из которых служит представителем своего класса эквивалентности.

2.3 Протоколы

Неформально говоря, протокол состоит из конечного множества участников, при этом каждый участник выполняет конечную фиксированную последовательность действий «приём–отправка». Как обычно в модели Долева–Яо, предполагается, что злоумышленник контролирует сеть: все сообщения, отправленные участником, сначала попадают к злоумышленнику, а все сообщения, которые получает участник, исходят от него. При получении сообщения от злоумышленника участник выполняет текущее действие «приём–отправка»: сначала проверяет и обрабатывает полученное сообщение, затем (если требуется) отправляет новое сообщение злоумышленнику. Следующее сообщение, полученное от злоумышленника, обрабатывается аналогичным образом на следующем шаге «приём–отправка».

Подобно другим моделям [21], мы описываем действия «приём–отправка» правилами переписи вида $R \quad \Rightarrow \quad S$, где R и S — термы. При получении сообщения m сначала проверяют, существует ли подстановка σ, такая что $\ulcorner m \urcorner = \ulcorner R\sigma \urcorner$. Если да, то в ответ участник формирует сообщение $\ulcorner S\sigma \urcorner$ и отправляет его злоумышленнику. Мы всегда предполагаем, что все сообщения, обмениваемые между участниками и злоумышленником, нормализованы. Следовательно, входящее m считается нормализованным, а результат применения правила записывается не просто как $S\sigma$, а как $\ulcorner S\sigma \urcorner$. Это отражает тот факт, что участники и злоумышленник не различают эквивалентные термы и работают только с их нормализованными представителями. Заметим также, что различные правила протокола могут разделять переменные, и некоторые из них в левой и правой частях правил могут уже быть связаны подстановками, порождёнными на предыдущих шагах.

Вместо того чтобы определять участников как последовательности правил переписи и протокол как множество участников, мы рассматриваем протокол как конечное частично упорядоченное множество правил переписи. Такая частичная упорядоченность допускает несколько линейных порядков, соответствующих разным последовательностям действий конкретных участников. Прежде чем перейти к строгому формальному определению протокола, рассмотрим пример.

Рассмотрим для примера протокол, задаваемый следующим набором правил:

$$\begin{aligned} 1: &\quad \text{Start} \;\Rightarrow\; N_a, \\ 2: &\quad \{N_a, x\}_K^s \;\Rightarrow\; \text{End}, \\ 1': &\quad y \;\Rightarrow\; \{y, N_b\}_K^s, \end{aligned}$$

с частичным порядком $1 < 2$. Интуитивно правила 1 и 2 описывают одно действие одного участника (Алисы), а правило $1'$ — действие другого участника (Боба). Частичный порядок гарантирует, что Алиса выполнит действие 1 перед действием 2, тогда как правило $1'$ может выполняться до 1, между 1 и 2 или после 2. Здесь N_a — одноразовое случайное значение, сгенерированный Алисой, N_b — одноразовое случайное значение Боба, а K — общий ключ между ними. Предполагается, что сообщение Start уже содержится в начальных знаниях злоумышленника.

Далее даётся формальное определение протоколов и правил переписи. В определение протокола также включаются начальные знания злоумышленника, поскольку именно атаки на протоколы нас интересуют далее (см. раздел 2.4). Три условия, предъявляемые к протоколам, будут объяснены сразу после формального определения.

Определение 2.6. Правило протокола имеет вид $R \;\Rightarrow\; S$, где R и S — стандартные термы.

Протокол P определяется как кортеж $\big(\{\, R_i \Rightarrow S_i \mid i \in I\}, \prec_I, E\big)$, где E — конечное нормализованное множество стандартных сообщений, называемое *начальными знаниями* злоумышленника, $\mathcal{I}$ — конечный (индексный) набор, $\prec_{\mathcal{I}}$ — частичный порядок на $\mathcal{I}$, для каждого $i \in \mathcal{I}$ правило $R_i \Rightarrow S_i$ является правилом протокола.

Протокол удовлетворяет следующим условиям: (1) Все стандартные термы R_i и S_i нормализованы.
(2) Для каждой переменной $x \in \mathcal{V}(S_i)$ существует $j \prec_{\mathcal{I}} i$ такое, что $x \in \mathcal{V}(R_j)$.
(3) Для каждого подтерма $Exp(t_1, t_2^{z_2} \cdots t_n^{z_n})$ в R_i существует $l \in \{1, \ldots, n\}$, $l \neq k$, такое, что

$$\mathcal{V}(t_l) \subseteq \bigcup_{j \prec_{\mathcal{I}} i} \mathcal{V}(R_j).$$

Далее для протокола P вводятся обозначения $\mathcal{A} := \{\text{константы, встречающиеся в } P\}$, $S(P) := E \cup \bigcup_{i \in I}\big(R_i \cup S_i\big)$, $\mathcal{V}(P) := V\big(S(P)\big)$. Размеры протокола определяются по размерам его подтермов: $|P| := \big|S(P)\big|$, $|P|_{\text{ext}} := \big|S(P)\big|_{\text{ext}}$, $\|P\| := \big\|S(P)\big\|$, $\|P\|_{\text{ext}} := \big\|S(P)\big\|_{\text{ext}}$.

Условие 1. Без ограничения общности, ввиду леммы 2.4 преобразование, выполняемое правилом протокола, и его нормализованный вариант совпадают.

Условие 2. Гарантирует, что при получении выходного сообщения в S_i все переменные в S_i уже «ограничены», то есть их подстановка определяется ранее принятыми от злоумышленника сообщениями. Иначе результат применения правила протокола мог бы быть произвольным, поскольку неограниченные переменные могли бы принять любое значение.

Условие 3. Гарантирует, что все показатели, за исключением, возможно, одного показателя t_k, в любом подтерме R_i вида $Exp(\cdot, \cdot)$ строятся на переменных с предыдущих шагов, то есть на переменных, которым были присвоены сообщения до i-го шага. Ниже мы покажем, что для недопущения пропуска атак спецификации протоколов не должны содержать переменных в показателях, значения которых не определены на предыдущих шагах. В этом смысле условие 3 можно было бы ужесточить, потребовав

$$\mathcal{V}(t_l) \subseteq \bigcup_{j \prec_I i} \mathcal{V}(R_j) \quad \text{для всех } l \in \{1, \ldots, n\},$$

в том числе для $l = k$. Однако мы пользуемся формулировкой (3) в определении 2.6, поскольку она достаточна и удобна для доказательств.

Обсуждение спецификации протоколов с экспоненцированием Диффи–Хеллмана. Обычно в протоколах, использующих экспоненцирование Диффи–Хеллмана, необходимо проверять, принадлежит ли данное сообщение определённой группе (например, [22]): принимается генератор группы g и сообщение m, после чего проверяется, существует ли сообщение (число) a такое, что $m = g^a$. В символической модели попытка смоделировать это оператором вида $Exp(g, x)$ (где g — константа, а x — переменная) будет в лоб совпадать только с сообщениями вида $Exp(g, m')$ для некоторых m', и тогда гарантированное сообщение принадлежности группе g исчезает. Так, если злоумышленник подаёт $Exp(b, m')$ или $Exp(\langle c, d\rangle, m')$ (при этом $\langle c, d\rangle$ может представлять битовую строку или элемент группы), то в криптографическом смысле сообщение не проходит проверку на членство: требуется тест на принадлежность группе. Однако в символическом мире эти сообщения совпадут с $Exp(g, x)$, и, соответственно, возможны атаки, несуществующие в реальной криптографии. Чтобы избежать таких «пропущенных» атак, предлагается в спецификациях протоколов вместо $Exp(g, x)$ использовать более общий шаблон $Exp(g, t)$, где t — некоторая переменная. То есть вместо записи $Exp(g, x) \rightarrow \ldots$ лучше писать $Exp(g, t) \rightarrow \ldots$ для некоторой переменной t. В такой символической записи автоматически принимаются все сообщения вида, например, $Exp(b, m')$ или $Exp(\langle c, d\rangle, m')$. Конечно, в криптографическом смысле такие сообщения в группе g не принадлежат, и такие атаки возможны. Тем не менее ясно, что в символической модели любую атаку на протокол, описанный без проверки членства, можно интерпретировать как атаку, независимую от конкретной группы, а проверку на членство можно вынести отдельно. Наконец, заметим, что наша модель исключает необходимость подстановки переменных нестандартными термами, поскольку сообщения вида $Exp(m, m')$ достаточно проверять на соответствие переменным.

2.4 Атаки

Теперь определим атаки на протоколы. Сначала введём понятие порядка исполнения протокола: это линейное упорядочение некоторого подмножества правил протокола, согласованное с заданным частичным порядком.

Определение 2.7. Пусть P — протокол с индексным множеством правил $\mathcal{I}$. Биективное отображение $\pi\colon \mathcal{I}' \to \{1,\ldots,p\}$ называется *порядком выполнения* протокола P, если $\mathcal{I}' \subseteq \mathcal{I}$, $p = |\mathcal{I}'|$, и для любых $i, j \in \mathcal{I}$ выполняется: если $i \prec_{\mathcal{I}} j$ и $\pi(j)$ определено, то $\pi(i)$ также определено и $\pi(i) < \pi(j)$. Размер порядка выполнения равен p.

Неформально говоря, в атаке на протокол P злоумышленник выбирает некоторый *порядок выполнения* протокола и затем пытается для каждого правила в этом порядке подобрать входные сообщения. Эти сообщения он выводит из своих начальных знаний и ранее полученных выходных сообщений. Цель злоумышленника — получить секретное сообщение. При анализе нескольких параллельно запущенных сеансов одного протокола они кодируются в рамках одного протокола P (bounded sessions), что обычно используется при ограничении числа сеансов (см. [21]).

Определение 2.8. Пусть $P = \big(\{\, R_i \Rightarrow S'_i \mid i \in \mathcal{I}\},\ \prec_{\mathcal{I}},\ S_0\big)$ — протокол. Тогда *атака* на P есть упорядоченная пара (π, σ), где π — порядок выполнения протокола P, а σ — нормализованная подстановка, такая что выполняются условия

(1) $\ulcorner R_i \urcorner \sigma^i \in \mathit{forge}\big(\ulcorner S_0,\ S_1\sigma,\ \ldots,\ S_{i-1}\sigma \urcorner\big)$ для каждого $i \in \{1,\ldots,k\}$, где $k = |\pi|,\ R_i = R'_{\pi^{-1}(i)},\ S_i = S'_{\pi^{-1}(i)}$;

(2) $\mathrm{secret} \in \mathit{forge}\big(\ulcorner S_0,\ S_1\sigma,\ \ldots,\ S_k\sigma \urcorner\big)$.

В силу леммы 2.4 неважно, нормализована ли подстановка в условии (1); достаточно требовать $\mathit{forge}(S_0, S_1\sigma, \ldots, S_{i-1}\sigma)$.

Рассматриваемая далее задача сводится к решению вопроса:

$$\mathsf{INSECURE} := \{\, P \mid \exists \text{ атака на } P\}.$$

Определение 2.9. Пусть $P = \big(\{\, R_i \Rightarrow S_i \mid i \in \mathcal{I}\},\ \prec_{\mathcal{I}},\ S_0\big)$ — протокол. Атака (π, σ) называется *минимальной*, если $|\sigma|$ минимально, то есть для любой другой подстановки σ', для которой (π, σ') является атакой на P, выполняется $|\sigma| \le |\sigma'|$.

Ясно, что если протокол небезопасен, то существует по крайней мере одна минимальная атака, хотя она может быть неединственной.

2.5 Оракульные правила

Оракульные правила — это угадывающие правила, удовлетворяющие дополнительным условиям. Для их определения введём несколько новых понятий.

Деривация D длины n ($n \geq 0$) есть последовательность шагов вида $E \rightarrow_{L_1} E, t_1 \rightarrow_{L_2} \cdots \rightarrow_{L_n} E, t_1 \cdots, t_n$ с конечным множеством стандартных сообщений E, стандартных сообщений $t_1 \cdots t_n$, а каждое $L_i \in \mathcal{L}$ удовлетворяет $E, t_1, \ldots, t_{i-1} \rightarrow_{L_i} E, t_1, \ldots, t_i$ и $t_i \notin E \cup \{t_1, \ldots, t_{i-1}\}$ для всех $i = 1, \ldots, n$. Правило L_i называется i-м правилом деривации D, а шаг $E, t_1, \ldots, t_{i-1} \rightarrow_{L_i} E, t_1, \ldots, t_i$ называется i-м шагом деривации. Пишем $L \in D$, если $L \in \{L_1, \ldots, L_n\}$. Если S — некоторое множество правил, то $S \notin D$ означает $S \cap \{L_1, \ldots, L_n\} = \emptyset$. Сообщение t_n называется *целью* деривации D.

Мы также нуждаемся в *корректных* деривациях, в которых каждое сообщение, получаемое на промежуточном шаге, либо уже содержится как подтерм в цели, либо принадлежит начальному множеству сообщений.

Определение 2.10. Пусть $D: \quad E \rightarrow_{L_1} \ldots \rightarrow_{L_n} E'$ — деривация с целью t. Тогда D называется *корректной*, если $E' \subseteq \mathcal{S}(E, t)$.

Теперь можно ввести оракульные правила. Первое условие в следующем определении позволит ограничить длину деривaций, оставшиеся — заменять подтерм u в подстановке σ на «меньшее» сообщение и затем использовать это при оценке размера σ в атаке.

Определение 2.11. Пусть $L_o = L_c \cup L_d$ — (конечное или бесконечное) множество угадывающих правил, где L_c и L_d — непересекающиеся множества правил композиции и разложения соответственно. Тогда L_o называется множеством *оракульных правил* (w.r.t. $L_c \cup L_d$) тогда и только тогда, когда выполнены все следующие условия:

Input: protocol $P = (\{R_\iota \Rightarrow S_\iota,\ \iota \in \mathcal{I}\}, <_\mathcal{I}, S_0)$. Recall that $\mathcal{V} = \mathcal{V}(P)$.

(1) Guess an execution ordering π for P. Let k, R_i, and S_i be defined as in Definition 2.8.
(2) Guess a normalized ground substitution σ such that $|\mathcal{V}\sigma| \leq |P|$ and $||\sigma||_{exp} \leq p(||P||)$.
(3) Test that $\ulcorner R_i\sigma \urcorner \in \mathit{forge}(\ulcorner \{S_j\sigma \mid j < i\} \cup \{S_0\} \urcorner)$ for every $i \in \{1, \ldots, k\}$.
(4) Test $\mathsf{secret} \in \mathit{forge}(\ulcorner \{S_j\sigma \mid j < k+1\} \cup \{S_0\} \urcorner)$.
(5) If each test is successful, then answer "yes", and otherwise, "no".

Рисунок 1 – NP-алгоритм для задачи INSECURE, где p обозначает полином, ограничивающий размер показателей произведений.

(1) Для любого сообщения t и любого конечного множества сообщений E, если $t \in \text{forge}(E) \implies$ тогда существует корректная деривация из E с целью t.
(2) Если $F \to_{L_{oc}(t)} F, t$ и $F, t \to_{L_{ad}(t)} F, t, a$, то существует деривация D из F с целью a, при этом $L_d(t) \notin D$.
(3) Для любого конечного множества сообщений F с $1 \in F$, если $F \setminus \{u\} \to_{\mathcal{L}_{oc}(u)} F$, то есть u может быть получено из $F \setminus \{u\}$ за один шаг, тогда из $F \to_{\mathcal{L}_{oc}(u)} F, t$ следует $\ulcorner t[u \leftarrow 1] \urcorner \in \text{forge}\big(\ulcorner F[u \leftarrow 1] \urcorner\big)$ для любого сообщения t.

3 NP-алоритм принятия решения

Теперь сформулируем одну из основных теорем этой работы, утверждающую, что задача INSECURE разрешима в классе NP для любого множества оракульных правил, удовлетворяющего двум условиям. Данная общая теорема будет применена в разделе 4 и разделе 7, чтобы показать, что INSECURE остаётся в NP в присутствии злоумышленника, способного выполнять экспоненцирование Диффи–Хеллмана и использовать коммутативное шифрование с открытым ключом, соответственно.

В теореме предъявляются два требования к множеству оракульных правил. Первое: проблема проверки применимости оракульного правила должна решаться эффективно. Второе: множество правил должно допускать полиномиальные атаки на показатели произведений.

Определение 3.1. Задача *oracle rule problem* задаётся как

$$\mathsf{OracleRule} \;=\; \{(E, m) \mid E \;\rightarrow_{L_o}\; E, m\},$$

где E — конечное нормализованное множество стандартных сообщений, а m — стандартное сообщение; оба подаются в виде DAG.

Говорят, что множество оракульных правил $\mathcal{L}_o$ *допускает полиномиальные атаки на показатели произведений*, если для любого протокола P и любой минимальной атаки (π, σ) на этот протокол существует подстановка σ' такая, что $\sigma' \approx \sigma$ (напомним, это означает совпадение σ' и σ с точностью до показателей произведений), пара $(\pi, \ulcorner\sigma'\urcorner)$ является атакой на P, и $\|\sigma'\|_{\exp}$ полиномиально ограничена по $\|P\|$. Заметим, что по лемме 2.4 из этого также следует полиномиальная ограниченность $\|\ulcorner\sigma'\urcorner\|$ по $\|P\|$.

Теорема 3.1. Пусть L_o — множество оракульных правил. Если

– $\mathsf{OracleRule} \in \mathsf{PTIME}$ и
– L_o допускает полиномиальные атаки на показатели произведений,

то задача INSECURE лежит в классе NP.

Теорема доказывается следующим образом. Сначала показывается, что недетермированный алгоритм из рисунка 1 является недетермированным полиномиальным алгоритмом и корректно решает задачу INSECURE. Полином p, ограничивающий размер показателей произведений, существует в силу того,

что L_o допускает полиномиальные атаки на показатели произведений. Структура алгоритма такова: на шагах 1 и 2 недетермированно выбирается «маленькая» атака (π, σ) на протокол P, а на шагах 3 и 4 проверяется, действительно ли (π, σ) является атакой на P.

Очевидно, что алгоритм из рисунка 1 корректен. Основная же сложность состоит в том, чтобы доказать полиномиальность его работы. Это делается с помощью результатов из разделов 3.1, 3.2 и 3.3. В дальнейшем мы сначала изложим эти результаты, а затем на их основе докажем полноту алгоритма и оценим его временную сложность.

В разделе 3.1 (см. теорему 3.2) показывается, что следующая задача, далее называемая *задачей вывода (derivation problem)*, решается за полиномиальное время от $\|E, t\|$, при условии, что OracleRule разрешима в детермированном полиномиальном времени:

$$\mathsf{Derive} \;:=\; \big\{(E, t) \mid t \in \mathrm{forge}(E)\big\},$$

где E — конечное множество стандартных сообщений, а t — стандартное сообщение, заданные в виде DAG.

В разделе 3.2 (см. утверждение 3.14) доказывается, что подстановки минимальных атак строятся из подтермов термов, встречающихся в описании протокола.

На основе предложения 3.14 в разделе 3.3 оценивается число подтермов в подстановках минимальных атак и выводится неравенство $|\sigma| \leq |P|$ (следствие 3.16).

Учитывая эти результаты, можем записать доказательство теоремы 3.1.

Доказательство теоремы 3.1. Покажем, что алгоритм из рисунка 1 работает в недетермированное полиномиальное время и является корректным и полным. Корректность уже была доказана.

Для доказательства полноты нужно убедиться, что если существует атака (π, σ) на протокол P, то найдётся атака с подстановкой σ', размер которой ограничен так, как это требуется в шаге 2 алгоритма из рисунка 1. Это немедленно следует из следствия 3.16 и предположения, что L_o допускает полиномиальные атаки на показатели произведений.

Остаётся показать, что наш алгоритм выполняется в недетермированное полиномиальное время по величине $\|P\|$. Для шагов 1 и 2 это очевидно. Чтобы убедиться в полиномиальности шагов 3 и 4, воспользуемся теоремой 3.2. Пусть $E = \{\ulcorner S_j\sigma \urcorner \mid j < i\} \cup \{\ulcorner S_0 \urcorner\}$ для некоторого $i \in \{1, \ldots, k\}$, а t обозначает либо $\ulcorner S_0 \urcorner$, либо *secret*. По теореме 3.2 проверка $t \in \mathit{forge}(E)$ может быть выполнена за детермированное полиномиальное время от $\|E, t\|$. По следствию 3.16 имеем $|E, t| \leq |P|$. Поскольку $\|\sigma\|_{\exp}$ полиномиально ограничено по $\|P\|$, то то же верно и для $\left\|\{\ulcorner S_j\sigma \urcorner \mid j < i\} \cup \{\ulcorner S_0 \urcorner\} \cup \{R_i\sigma\}\right\|_{\exp}$. По лемме 2.4 из этого следует, что $\|E, t\|_{\exp}$ полиномиально ограничено по $\|P\|$. Следовательно, шаги 3 и 4 могут быть выполнены за детермированное полиномиальное время по $\|P\|$. $\square$

3.1 Решение задачи вывода

Покажем, что задачу вывода (derivation problem) можно решить за полиномиальное время, при условии, что задача OracleRule разрешима в детермированном полиномиальном времени.

Теорема 3.2. Задача

$$\mathsf{Derive} := \{(E, t) \mid t \in \mathrm{forge}(E)\}$$

разрешима в классе PTIME, при условии, что $\mathsf{OracleRule} \in \mathsf{PTIME}$.

Доказательство. Пусть $d_t(E) = \{\, t' \in S(E, t) \mid E \to_{L_o} E, t' \}$ — множество сообщений t', выводимых из E за один шаг. Поскольку число таких t' линейно по $\|E, t\|$, а проверка шага $E \to_{L_o} E, t'$ выполняется за детермированное полиномиальное время от $\|E, t\|$, нетрудно убедиться, что $d_t(E)$ вычисляется за полиномиальное время от $\|E, t\|$. Теперь предположим, что $t \in \mathrm{forge}(E)$. По определению 2.11 существует корректная деривация $D : E \to_{L_1} E, t_1 \to \ldots \to_{L_r} E, t_1, \ldots, t_r$, где $t_r = t$. В частности, $t_i \in S(E, t)$ при $i = 1, \ldots, r$, и все t_i попарно различны, поэтому $r \leq |E, t|$. Введём рекурсию $d_t^0(E) := E$, $d_t^{i+1}(E) := d_t\big(d_t^i(E)\big)$. Очевидно, что $t \in d_t^r(E) \iff t \in \mathrm{forge}(E)$. Поскольку каждый шаг вычисления $d_t^i(E)$ занимает полиномиальное время от $\|E, t\|$, вытекает, что проверка $t \in \mathrm{forge}(E)$ также выполняется за детермированное полиномиальное время. $\square$

3.2 Характеризация подтермов минимальных атак

Далее мы покажем, что подстановки минимальных атак могут быть сконструированы путём «связывания» подтермов, которые изначально встречаются в спецификации задачи (см. Утверждение 3.14). Для доказательства этого утверждения сначала установим некоторые свойства замен (Леммы 3.4–3.6), затем свойства подстановок в минимальных атаках (Леммы 3.7–3.9) и, наконец, свойства дериваций (Леммы 3.10–3.13).

В дальнейшем мы всегда предполагаем, что L_o — множество оракульных правил. Если $t \in \text{forge}(E)$, то обозначим через $D_t(E)$ некоторую корректную деривацию из E с целью t (выбранную произвольно). Такая деривация всегда существует в силу определения оракульных правил.

Пусть $P = \big(\{\, R_i \Rightarrow S_i \mid i \in \mathcal{I}\},\ \prec_{\mathcal{I}},\ S_0\big)$ — протокол, а (π, σ) — атака на P. Пусть $k = |\pi|$, а R_i и S_i определены согласно Определению 2.8. Напомним, что $S(P) = S_0 \cup \bigcup_{i\in\mathcal{I}}(R_i \cup S_i)$, $\mathcal{V}(P) = \mathcal{V}\big(S(P)\big)$. Также нам понадобится следующее ключевое понятие.

Определение 3.3. Пусть t и t' — два терма, а θ — наземная подстановка. Тогда говорят, что t является θ-соответствием (или θ-match) терма t', что обозначается

$$t \sqsubseteq_\theta t',$$

если t и t' — стандартные термы и

$$\ulcorner t\,\theta \urcorner = t'.$$

3.2.1 Свойства замен

Следующие леммы устанавливают дистрибутивные свойства функции нормализации, подстановок, оператора экспоненцирования и операций замены.

Лемма 3.4. Пусть u — нормализованный терм, а M, M' — два произведения, такие что все подтермы из $\mathcal{F}(M) \cup \mathcal{F}(M')$ нормализованы. Пусть s — стандартный нормализованный терм, а $\delta = [s \leftarrow 1]$ — замена. Тогда выполняются равенства:

(1) $\ulcorner (M \cdot M')\delta \urcorner = \ulcorner\ulcorner M \cdot M' \urcorner \delta \urcorner$, в частности $\ulcorner M\delta \urcorner = \ulcorner\ulcorner M \urcorner \delta \urcorner$.

(2) $\ulcorner Exp(u, M)\delta \urcorner = \ulcorner\ulcorner Exp(u, M) \urcorner \delta \urcorner$, если $s \neq \ulcorner Exp(u, M) \urcorner$, и, в случае если $s = Exp(\cdot, \cdot)$, также $s \neq u$.

Доказательство. См. Приложение А □

Отметим, что пункт 2 в предыдущей лемме не выполняется без ограничений на s. Следующий пример демонстрирует проблему при $s = \ulcorner Exp(u, M)\urcorner$: предположим, что $s = Exp(a, b)$, $u = a$, а $M = b \cdot c \cdot c^{-1}$. Тогда $s = \ulcorner Exp(u, M)\delta\urcorner \neq \ulcorner\ulcorner Exp(u, M)\urcorner\delta\urcorner = 1$. Следующий пример иллюстрирует, почему необходимо требование $s \neq u$: положим $s = u = Exp(a, b)$ и $M = c$. Тогда $1 = \ulcorner Exp(u, M)\delta\urcorner \neq \ulcorner\ulcorner Exp(u, M')\urcorner\delta\urcorner = Exp(a, b{\cdot}c)$.

Лемма 3.5. Пусть σ — нормализованная замкнутая подстановка, E — множество нормализованных термов, s — нормализованный стандартный неатомарный терм, а δ — замена $[s \leftarrow 1]$. Обозначим $\sigma' = \ulcorner\sigma\delta\urcorner$. Если не существует стандартного подтерма $t \in E$ такого, что $t \sqsubseteq_\sigma s$, то $\ulcorner E\sigma'\urcorner = \ulcorner\ulcorner E\sigma\urcorner\delta\urcorner$.

Доказательство. См. Приложение А. □

Лемма 3.6. Пусть $t', t_1, \ldots, t_n, t, u$ — нормализованные стандартные термы, $z_1, \ldots, z_n \in \mathbb{Z}$, а δ — замена $[u \leftarrow 1]$ такая, что $u \neq t$ и $t = \ulcorner Exp\big(t',\, t_1^{z_1} \cdots t_n^{z_n}\big)\urcorner$. Если $t' = Exp(\,\cdot, \cdot\,)$, то дополнительно предполагаем $u \neq t'$. Тогда

$$\ulcorner t\delta\urcorner = \ulcorner Exp\big(\ulcorner t'\delta\urcorner, \ulcorner t'\delta\urcorner^{z_1} \cdots \ulcorner t_n\delta\urcorner^{z_n}\big)\urcorner.$$

Доказательство. См. Приложение А. □

3.2.2 Свойства подстановок минимальных атак

Следующая лемма позволяет доказать то, что мы далее будем называть *свойством единственного сопоставления.*

Лемма 3.7. Пусть s — стандартный терм, t — нормализованный терм, а σ — нормализованная подстановка такая, что $s \in S(\ulcorner t\sigma\urcorner)$ и $s \notin S(x\sigma)$ для каждого $x \in \mathcal{V}(t)$. Тогда существует стандартный подтерм t' терма t, удовлетворяющий $t' \sqsubseteq_\sigma s$.

Доказательство. По лемме 2.4 имеем

$$S(\ulcorner t\sigma\urcorner) \;\subseteq\; \ulcorner S(t\sigma)\urcorner \;\subseteq\; \ulcorner S(t)\sigma \;\cup\; \mathcal{V}(t)\sigma\urcorner.$$

Так как σ находится в нормальной форме, это означает

$$S(\ulcorner t\sigma\urcorner) \;\subseteq\; \ulcorner S(t)\sigma\urcorner \;\cup\; \mathcal{V}(t)\sigma.$$

По предположению $s \in \mathcal{S}(\ulcorner t\sigma \urcorner)$ и $s \notin \mathcal{S}(\mathcal{V}(t)\sigma)$. Следовательно, $s \in \ulcorner \mathcal{S}(t)\sigma \urcorner$, то есть существует $t' \in \mathcal{S}(t)$ такое, что $\ulcorner t'\sigma \urcorner = s$. □

Теперь мы докажем *свойство единственного сопоставления*: если злоумышленник посылает сообщения $m_1, \ldots, m_i$, то существует не более одного способа сопоставить эти сообщения с $R_1, \ldots, R_i$ при каждом $R_j,\ j \in \{1, \ldots, i\}$, определённых выше.

Лемма 3.8. *Пусть дана произвольная последовательность нормализованных сообщений $m_1, \ldots, m_i$. Существует не более одной нормализованной подстановки σ такой, что $\ulcorner R_j\sigma \urcorner = m_j$ для всех $j \in \{1, \ldots, i\}$.*

Доказательство. Предположим противное и выберем минимальный $i \in \{1, \ldots, n\}$, для которого существуют две разные нормализованные подстановки σ и σ', удовлетворяющие $\ulcorner R_j\sigma \urcorner = \ulcorner R_j\sigma' \urcorner$ для всех $j \in \{1, \ldots, i\}$. Из минимальности i следует, что σ и σ' совпадают на $V_{i-1} = \mathcal{V}(R_1, \ldots, R_{i-1})$ и различаются на некоторой переменной из $\mathcal{V}(R_i) \setminus V_{i-1}$. Обозначим через σ_0 подстановку, равную σ на V_{i-1} и тождественную на $\mathcal{V}(R_i) \setminus V_{i-1}$; положим $r = \ulcorner R_i\sigma_0 \urcorner$.

По Лемме 2.4, 5 и поскольку $R_i\sigma = (R_i\sigma_0)\sigma$ и $R_i\sigma' = (R_i\sigma_0)\sigma'$, получаем $\ulcorner R_i\sigma \urcorner = \ulcorner r\sigma \urcorner = \ulcorner r\sigma' \urcorner$. По предположению найдётся переменная $x \in \mathcal{V}(r)$ такая, что $x\sigma \neq x\sigma'$. Выберем $t_x \in \mathcal{S}(r)$ минимальный (относительно отношения «подтерм»), для которого $x \in \mathcal{V}(t_x)$ и $\ulcorner t_x\sigma \urcorner = \ulcorner t_x\sigma' \urcorner$. Так как r является возможным кандидатом, такой терм t_x корректно определён.

Очевидно, t_x не может быть ни переменной, ни константой. На самом деле легко видеть, что t_x обязан иметь вид $Exp(t_1, t_2^{z_2} \cdots t_k^{z_k})$. По Определению 2.6, 3 и так как $x \in \mathcal{V}(t_x)$, для всех $j \in \{1, \ldots, k\} \setminus \{j_0\}$ термы t_j являются замкнутыми. Пусть j_0 — индекс незамкнутого подтерма, т. е. $x \in \mathcal{V}\big(t_{j_0}\big)$. По минимальности t_x имеем $t_{j_0}\sigma \neq t_{j_0}\sigma'$. Учитывая, что $t_x\sigma = t_x\sigma'$, рассмотрим возможные случаи:

— $j_0 = 1$: Сначала предположим, что $\ulcorner t_{j_0}\sigma \urcorner = Exp(b, M)$ и $\ulcorner t_{j_0}\sigma' \urcorner = \mathrm{Exp}(b', M')$. Так как $\ulcorner t_x\sigma \urcorner = \ulcorner t_x\sigma' \urcorner$, имеем $b = b'$ и $\ulcorner M \cdot \prod_{i=2}^{k} t_i^{z_i} \urcorner = \ulcorner M' \cdot \prod_{i=2}^{k} t_i^{z_i} \urcorner$. Отсюда $M = M'$ и, следовательно, $\ulcorner t_{j_0}\sigma \urcorner = \ulcorner t_{j_0}\sigma' \urcorner$, что противоречит предположению. Если оба терма $\ulcorner t_{j_0}\sigma \urcorner$ и $\ulcorner t_{j_0}\sigma' \urcorner$ не имеют вида $\mathrm{Exp}(\,\cdot, \cdot\,)$, то из равенства $\ulcorner t_x\sigma \urcorner = \ulcorner t_x\sigma' \urcorner$ также немедленно следует $\ulcorner t_{j_0}\sigma \urcorner = \ulcorner t_{j_0}\sigma' \urcorner$. Если же $\ulcorner t_{j_0}\sigma \urcorner = \mathrm{Exp}(b, M)$, а $\ulcorner t_{j_0}\sigma' \urcorner$ не имеет вида $\mathrm{Exp}(\,\cdot, \cdot\,)$, то равенство $\ulcorner t_x\sigma \urcorner = \ulcorner t_x\sigma' \urcorner$ влечёт $\ulcorner M \cdot \prod_{i=2}^{k} t_i^{z_i} \urcorner = \ulcorner \prod_{i=2}^{k} t_i^{z_i} \urcorner$, а значит $M = 1$, что противоречит тому, что $t_{j_0}\sigma$ нормализован. Следовательно, случай $j_0 = 1$ невозможен.

— $j_0 > 1$: Сначала предположим, что $t_1 = Exp(b, M)$. Из равенства $\ulcorner t_x\sigma \urcorner = \ulcorner t_x\sigma' \urcorner$ получаем

$$\ulcorner M \cdot \ulcorner t_{j_0}^{z_{j_0}}\sigma \urcorner \cdot \prod_{j\in\{2,\dots,k\}\setminus\{j_0\}} \big(t_j\big)^{z_j} \urcorner \;=\; \ulcorner M \;\cdot\; \ulcorner t_{j_0}^{z_{j_0}}\sigma' \urcorner \;\cdot \prod_{j\in\{2,\dots,k\}\setminus\{j_0\}} t_j^{z_j} \urcorner$$

Следует $\big(t_{j_0}\sigma\big)^{z_{j_0}} = \big(t_{j_0}\sigma'\big)^{z_{j_0}}$, что противоречит выбору t_{j_0}. Случай, когда $t_x\sigma$ не имеет вида $\mathrm{Exp}(\,\cdot,\cdot\,)$, разбирается ещё проще. □

Используя предыдущую лемму, покажем, что любой подтерм подстановки, соответствующей минимальной атаке, либо принадлежит спецификации протокола, либо является подтермом нормализованного сообщения, передаваемого в ходе атаки.

Лемма 3.9. Пусть (π, σ) — атака на P с нормализованной подстановкой σ, $x \in \mathcal{V}(R_i)$ для некоторого $i \in \{1, \dots, k\}$, а $s \in \mathcal{S}\big(\sigma(x)\big)$ — стандартный терм. Тогда существует $j \le i$ такое, что $s \in \mathcal{S}\big(\ulcorner R_j\sigma \urcorner\big)$ или существует $t \in S(P)$ со свойством $t \sqsubseteq_\sigma s$.

Доказательство. Предположим, что не существует $t \in S(P)$ такого, что $t \sqsubseteq_\sigma s$, и при этом $s \notin S\big(\ulcorner R_j\sigma \urcorner\big)$ для всех $j \le i$. Отсюда s не является атомом. Положим $V_j = \mathcal{V}(R_j) \cup \mathcal{V}(S_j)$ и выберем минимальный j, для которого $s \in S\big(V_j\sigma\big)$. По Определению 2.6, 2 имеем $s \in S\big(\mathcal{V}(R_j)\sigma\big)$. Обозначим $\sigma' = \ulcorner \sigma[s \leftarrow 1] \urcorner$.

По минимальности j для всех $l < j$ выполняется $R_l\sigma' = R_l\sigma$, а значит $\ulcorner R_l\sigma' \urcorner = \ulcorner R_l\sigma \urcorner$. Поскольку $s \notin S\big(\ulcorner R_j\sigma \urcorner\big)$, получаем $\ulcorner R_j\sigma' \urcorner[s \leftarrow 1] = \ulcorner R_j\sigma \urcorner$. По Лемме 3.5 отсюда следует $\ulcorner R_j\sigma \urcorner = \ulcorner R_j\sigma' \urcorner$. Заметим, что σ и σ' различаются хотя бы по одной переменной из $\mathcal{V}(R_1, \dots, R_j)$, что противоречит Лемме 3.8. □

3.2.3 Свойства выводов

Ниже приводятся несколько полезных свойств выводов, позволяющих без труда заменять термы внутри вывода. Начнём с простого наблюдения, непосредственно вытекающего из определения правил декомпозиции и композиции.

Лемма 3.10. Пусть E — нормализованное конечное множество сообщений, t — сообщение, а L — t-правило, для которого выполнен один шаг вывода $E \to_L E, t$, и при этом $\mathcal{S}(E, t) \neq \mathcal{S}(E)$. Тогда $\mathcal{S}(E, t) = \mathcal{S}(E) \cup \{t\}$, и L является правилом композиции.

Следующая лемма утверждает, что если t' — подтерм терма t, терм t выводится из множества E, но при этом t' не является подтермом ни одного элемента E, то t' также выводится из E, причём последним шагом такого вывода служит правило композиции.

Лемма 3.11. Предположим, что $t' \in \mathcal{S}(t) \setminus \mathcal{S}(E)$ и $t \in forge(E)$. Тогда $t' \in forge(E)$, и существует вывод из E с целью t', завершающийся правилом композиции.

Доказательство. Пусть $D = E_0 \to_{L_1} E_1 \cdots \to_{L_n} E_n$ — вывод терма t, причём $E_0 = E$. Так как t' является подтермом элементов E_n, существует минимальный $i > 0$ такой, что $t' \in \mathcal{S}(E_i)$. По минимальности i имеем $t' \in \mathcal{S}(E_i) \setminus \mathcal{S}(E_{i-1})$. Применяя Лемму 3.10, заключаем, что $D = E_0 \to_{L_1} E_1 \cdots \to_{L_i} E_i$ — это вывод с целью t'. □

Следующая лемма будет использована в доказательстве Леммы 3.13. Она позволяет строить специальные выводы, в которых заданный терм никогда не декомпозируется. Это окажется критически важным, когда потребуется заменить составные термы атомами в ряде выводов.

Лемма 3.12. Пусть $t \in forge(E)$ и $\gamma \in forge(E)$. Предположим, что имеется вывод D_γ из E, последним шагом которого является применение правила из $\mathcal{L}_c$. Тогда существует вывод D' из E с целью t, удовлетворяющий $L_d(\gamma) \notin D'$.

Доказательство. См. Приложение А. □

Теперь мы можем сформулировать лемму, позволяющую заменять определённые подтермы, возникающие в подстановке атаки, на более короткие. Из предположений текущей леммы следует, что s выводим из E так, что последним правилом является правило композиции. Это даёт возможность заменить s на более короткий терм, поскольку при выводе t декомпозиция s уже не потребуется.

Лемма 3.13. Пусть E и F — два множества нормализованных сообщений, причём $1 \in E \cup F$. Пусть $t \in forge(E, F)$ и $s \in forge(E)$ — неатомарный терм, причём $s \notin \mathcal{S}(E)$. Обозначим через δ подстановку $[\, s \leftarrow 1 \,]$. Тогда $\ulcorner t\delta \urcorner \in forge\big(\ulcorner E\delta, F\delta \urcorner\big)$.

Доказательство. По лемме 3.11 существует корректный вывод D_s из E с целью s, в котором последний шаг — правило композиции. По лемме 3.12 имеется вывод D_t из E, F с целью t, такой, что $L_d(s) \notin D_t$. Запишем $D_t : \quad E, F \to_{L_1} E, F, t_1 \to_{L_2} E, F, t_2 \ \cdots \ \to_{L_n} E, F, t_1, \ldots, t_n$.

Покажем по индукции по i $(0 \le i \le n)$, что

$$\ulcorner t_i\delta \urcorner \ \in \ forge\big(\ulcorner E\delta,\, F\delta \urcorner\big).$$

База. Если $t_0 \in E \cup F$, то $\ulcorner t_0\delta \urcorner \in \ulcorner E\delta \cup F\delta \urcorner \subseteq forge\big(\ulcorner E\delta,\, F\delta \urcorner\big)$.

Индукционный шаг. Пусть утверждение доказано для всех $j < i$; рассмотрим правило L_i.

– $L_i = L_c(\langle a, b\rangle)$: либо $t_i = s$ и тогда $t_i\delta = 1 \in forge(E\delta, F\delta)$, либо $t_i\delta = \langle a\delta, b\delta\rangle$. По предположению индукции $\{a\delta, b\delta\} \subseteq forge\big(\ulcorner E\delta,\, F\delta \urcorner\big)$, откуда $t_i\delta \in forge\big(\ulcorner E\delta,\, F\delta \urcorner\big)$. Аналогично разбираются случаи $\{a\}^s_b$ и $\{a\}^p_K$.

– $L_i = L_{p1}(\langle t_i, a\rangle)$: здесь $s \ne \langle t_i, a\rangle$, так как $L_i \notin L_d(s)$. Получаем $\langle t_i, a\rangle\delta = \langle t_i\delta, a\delta\rangle$. По индукционной гипотезе $\langle t_i, a\rangle\delta \in forge(E\delta, F\delta)$, следовательно $t_i\delta \in forge(E\delta, F\delta)$. Точно так же обрабатываются правила L_{p2}, L_{sd} и L_{ad}.

– $L_i \in L_o$: воспользуемся Определением 2.11, 3. Пусть E' — множество сообщений, полученное в D_s непосредственно перед применением последнего шага. Тогда $E' \setminus \{s\} \to_{\mathcal{L}_c(s)} E', s$, а также

$$E, F, t_1, \ldots, t_{i-1} \to_{L_i} E, F, t_1, \ldots, t_i.$$

В частности, $E', E, F, t_1, \ldots, t_{i-1} \ \to_{L_i} \ E', E, F, t_1, \ldots, t_{i-1}, t_i$, откуда по Определению 2.11, 3

$$\ulcorner t_i\delta \urcorner \in forge\big(\ulcorner E'\delta,\, E\delta,\, F\delta,\, t_1\delta, \ldots, t_{i-1}\delta \urcorner\big).$$

Заметим, что $E'\delta = E'$, $E\delta = E$, а все сообщения из E' выводимы из E. Индукционное предположение даёт $\ulcorner t_1\delta \urcorner, \ldots, \ulcorner t_{i-1}\delta \urcorner \in forge\big(\ulcorner E\delta,\, F\delta \urcorner\big)$, поэтому $forge\big(\ulcorner E'\delta,\, E\delta,\, F\delta,\, t_1\delta, \ldots, t_{i-1}\delta \urcorner\big) \subseteq forge\big(\ulcorner E\delta,\, F\delta \urcorner\big)$, и поэтому $t_i\delta \in forge\big(\ulcorner E\delta,\, F\delta \urcorner\big)$.

Для $i = n$ получаем $t\delta \in forge(E\delta, F\delta)$, что и требовалось. $\square$

3.2.4 Свойства минимальных атак

Теперь мы готовы перейти к доказательству Предложения 3.14, которое утверждает, что подстановки минимальных атак всегда можно построить, связывая подтермы, изначально присутствующие в протоколе P. Это ключевой шаг, позволяющий ограничить число подтермов в минимальных атаках (см. Теорему 3.15).

Предложение 3.14. Пусть (π, σ) — минимальная атака на протокол P. Тогда для любого $s \in S(\mathcal{V}\sigma)$ существует $t \in \mathcal{S}(P)$ такое, что $t \sqsubseteq_\sigma s$.

Доказательство. Положим (π, σ) и s как выше. Предположим обратное (*): *для каждого* t *из условия* $t \sqsubseteq_\sigma s$ *следует* $t \notin \mathcal{S}(P)$. Доведём это допущение до противоречия.

Так как $\mathcal{A} \subseteq \mathcal{S}(P)$, получаем $s \notin \mathcal{A}$. По лемме 3.9 и (*) существует j такое, что $s \in \mathcal{S}\big(\ulcorner R_j\sigma \urcorner\big)$. Выберем минимальный среди возможных j и рассмотрим $N = j$. Если $s \in \mathcal{S}\big(\ulcorner S_i\sigma \urcorner\big)$ для некоторого i, то (*) и лемма 3.7 дают нам переменную $x \in \mathcal{V}(S_i)$ с $s \in S(x\sigma)$. По определению 2.6, (2) существуют $R_{i'}, i' \le i$ такие, что $x \in \mathcal{V}(R_k)$. Следовательно, леммы 3.9 и (*) вновь дают индекс $j \le i$ с $s \in S\big(\ulcorner R_j\sigma \urcorner\big)$. Заметим, что $s \notin \mathcal{S}(S_0)$, иначе $s \in \mathcal{S}(P)$, и (*) бы не выполнялось. Минимальность N гарантирует $i \ge N$. Положим $E_j = \ulcorner S_0\sigma, \ldots, S_{j-1}\sigma \urcorner$. Итак, s — неатомарный терм, не являющийся подтермом E_N, но являющийся подтермом $\ulcorner R_N\sigma \urcorner$; по лемме 3.11 тогда $s \in forge(E_N)$.

Обозначим $\delta = [\, s \leftarrow 1 \,]$. Поскольку (π, σ) — атака, для всех $1 \le j \le k+1$ (где $R_{k+1} = \mathit{secret}$) выполняется

$$\ulcorner R_j\sigma \urcorner \;\in\; forge(E_j).$$

Рассмотрим два случая.

— $j < N$. Минимальность N означает, что s не является подтермом ни $\ulcorner R_j\sigma \urcorner$, ни E_j. Тогда из $\ulcorner R_j\sigma \urcorner \in forge(E_j)$ получаем $\ulcorner\ulcorner R_j\sigma \urcorner\delta \urcorner \in forge\big(\ulcorner E_j\delta \urcorner\big) = forge(E_j\delta)$.

— $j \ge N$. Полагая $t = \ulcorner R_j\sigma \urcorner$, $E = E_N$, $F = E_j$, применяем лемму 3.13 и получаем $\ulcorner\ulcorner R_j\sigma \urcorner\delta \urcorner \in forge\big(\ulcorner E_j\delta \urcorner\big)$.

Таким образом, $\ulcorner\ulcorner R_j\sigma\urcorner\delta\urcorner \in forge(\ulcorner E_j\delta\urcorner)$ в обоих случаях. Теперь из (*) и леммы 3.5 для всех j выводим

$$\ulcorner R_j\sigma\urcorner \in forge\big(\ulcorner S_0\sigma', \ldots, S_{j-1}\sigma'\urcorner\big), \qquad \text{где } \sigma' = \ulcorner\sigma\delta\urcorner.$$

Следовательно, (π, σ') также является атакой. (Условия применения леммы 3.5 выполнены.) Но σ' получена из σ заменой s на терм 1, то есть $|\sigma'| < |\sigma|$, что противоречит минимальности атаки (π, σ). □

3.3 Ограничение числа подтермов минимальных атак

Опираясь на Предложение 3.14, получаем:

Теорема 3.15. Для каждой минимальной атаки (π, σ) на протокол P выполнено

$$\mathcal{S}\big(\ulcorner\mathcal{S}(P)\sigma\urcorner\big) \;=\; \ulcorner\mathcal{S}(P)\sigma\urcorner.$$

Доказательство. Включение $\ulcorner\mathcal{S}(P)\sigma\urcorner \subseteq S\big(\ulcorner\mathcal{S}(P)\sigma\urcorner\big)$ очевидно. Обратное включение является прямым следствием Предложения 3.14, из которого получаем

$$\mathcal{S}(\mathcal{V}\sigma) \subseteq \ulcorner\mathcal{S}(P)\sigma\urcorner.$$

По лемме 2.4 имеем $S\big(\ulcorner\mathcal{S}(P)\sigma\urcorner\big) \subseteq \ulcorner\mathcal{S}\big(\mathcal{S}(P)\sigma\big)\urcorner$, $\quad \mathcal{S}\big(\mathcal{S}(P)\sigma\big) \subseteq \mathcal{S}(P)\sigma \;\cup\; \mathcal{S}(\mathcal{V}\sigma)$. Следовательно, $\mathcal{S}\big(\ulcorner\mathcal{S}(P)\sigma\urcorner\big) \subseteq \ulcorner\mathcal{S}(P)\sigma\urcorner \cup \mathcal{S}(\mathcal{V}\sigma)$, и, учитывая предыдущее включение, получаем $S\big(\ulcorner S(P)\sigma\urcorner\big) \subseteq \ulcorner S(P)\sigma\urcorner$. Тем самым равенство доказано. □

Из Теоремы 3.15 немедленно следует:

Следствие 3.16. Для каждой минимальной атаки (π, σ) на протокол P и любого множества $E \subseteq \mathcal{S}(P)$ выполняется $\big|\ulcorner E\sigma\urcorner\big| \;\leq\; |P|$. В частности, $|\,\mathcal{V}(P)\sigma| \;\leq\; |P|$.

Доказательство. Во-первых, мощность множества $\mathcal{S}\big(\ulcorner\mathcal{S}(P)\sigma\urcorner\big)$ не превышает $|P|$. Во-вторых, $\ulcorner E\sigma\urcorner \;\subseteq\; \mathcal{S}\big(\ulcorner\mathcal{S}(P)\sigma\urcorner\big)$, откуда сразу следует требуемое $\big|\ulcorner E\sigma\urcorner\big| \leq |P|$. Подставляя $E = \mathcal{V}(P)$, получаем $|\,\mathcal{V}(P)\sigma| \leq |P|$. Заметим, что σ нормализована, поэтому $\sigma(x) = \ulcorner\sigma(x)\urcorner$ для любой переменной x. □

4 Расширение модели нарушителя Долева–Яо за счёт экспоненцирования Диффи–Хеллмана

Мы расширяем нарушителя Долева–Яо, определённого правилами $L_c \cup L_d$ (см. п. 2.2), добавляя набор правил L_σ — *DH-правила*, позволяющих нарушителю выполнять экспоненцирование Диффи–Хеллмана. Расширенный нарушитель будем называть *DH-нарушителем*. Наша цель — показать, что для DH-нарушителя задача вывода решается за детермированное полиномиальное время, а задача небезопасности решается за недетермированное полиномиальное время. Для этого проверим, что выполняются предпосылки Теоремы 3.2 и Теоремы 3.1. Напомним, Теорема 3.2 требует:

а) L_σ является множеством оракульных правил и

б) OracleRule решается за полиномиальное время;

дополнительно Теорема 3.1 требует:

а) L_σ допускает полиномиальные «произведение-показатель»-атаки.

В разделах 4.1 и 4.2 мы докажем пункт а), а в разделе 4.3 — пункт б). Используя Теорему 3.2, придём к выводу, что для DH-нарушителя задача вывода решается за полиномиальное время (см. Следствие 4.9).

В разделе 5 мы докажем пункт iii); совместно с Теоремой 3.1 это даст, что для DH-нарушителя задача небезопасности решается за недетермированное полиномиальное время (см. Теорему 5.23).

Сначала зададим DH-правила L_σ.

Определение 4.1 (4.1)**.** Положим $L_\sigma = L_{\sigma_c} \cup L_{\sigma_d}$, где L_σ состоит из всех правил вида

$$t,\, t_1, \ldots, t_n \;\longrightarrow\; \ulcorner Exp\big(t, t_1^{z_1} \cdots t_n^{z_n}\big) \urcorner \;=:\; u,$$

где $n \geq 1$, $z_i \in \mathbb{Z} \setminus \{0\}$, $1 \leq i \leq n$, а $t, t_1, \ldots, t_n$ — нормализованные стандартные сообщения. Если u имеет вид $Exp(\cdot, \cdot)$, то правило входит в $L_{\sigma_c}(u)$ (множество *композиционных* DH-правил); иначе — в $L_{oc}(u)$ (множество *декомпозиционных* DH-правил). Нарушителя, использующего L_0 как оракульные правила, мы называем *DH-нарушителем*. Терм t в правиле называют *головой* правила, а $z_1, \ldots, z_n$ — *показателями произведения*. Будем считать без ограничения общности, что голова декомпозиционного DH-правила имеет форму $Exp(\cdot, \cdot)$ (иначе $t = u$); также полагаем $t_i \neq t_j$ при $i \neq j$ и $z_i \neq 0$ для всех i.

Так как сообщения в правой части DH-правила нормализованы, легко получить следующее.

Лемма 4.2. Правила из L_{oc} являются композиционными, а правила из L_{od} — декомпозиционными правилами угадывания.

4.1 Диффи–Хеллман правила допускают корректные выводы

Покажем, что L_o допускает корректные выводы (лемма 4.5). Иными словами, L_o удовлетворяет первому из требований к «oracle-rules» (см. определение 2.11). Доказательство опирается на две вспомогательные леммы, приведённые ниже.

Первая лемма позволяет ограничиться такими выводами, в которых правила из L_o применяются только к тем сообщениям, которые были либо созданы правилами Долева–Яо (DH), либо присутствовали в исходном множестве сообщений.

Лемма 4.3. Пусть E — конечное множество нормализованных стандартных сообщений, t — стандартное сообщение такое, что t выводится из E (относительно L). Пусть D — вывод из E с целью t. Тогда существует вывод D' из E с той же целью t, удовлетворяющий:

а) D' имеет ту же длину, что и D;

б) для любого DH-правила $L \in D' \cap L_o$ с головным термом t' выполнено: $t' \in E$ или существует t'-правило $L' \in D' \cap (L_d \cup L_c)$. Более того, если L — *декомпозиционное* DH-правило, то $t' \in E$ или существует t'-правило $L' \in D' \cap L_d$.

Доказательство. См. Приложение Б. □

Следующая лемма даёт критерий, позволяющий проверить, корректен ли вывод.

Лемма 4.4. Пусть $D = E_0 \to_{L_1} \dots E_{n-1} \to_{L_n} E_n$ — вывод с целью g.

а) Предположим, что для каждого шага $E_{j-1} \to L_j\, E_j$ вывода D с $L_j \in \mathcal{L}_d(t)$ существует $t' \in E_{j-1}$ такое, что $t \sqsubseteq t'$ и $t' \in E_0$ или $\exists\, i < j : L_i \in \mathcal{L}_d(t')$. Тогда из $L \in D \cap \mathcal{L}_d(t)$ (для некоторого $\mathcal{L}, t$) следует $t \in \mathcal{S}(E_0)$.

б) Предположим, что для каждого $i < n$ и t с $L_i \in \mathcal{L}_c(t)$ найдётся $j > i$ такое, что L_j является t'-правилом и $t \in \mathcal{S}\big(\{t'\} \cup E_0\big)$. Тогда из $L \in D \cap \mathcal{L}_c(t)$ (для некоторого L, t) следует $t \in \mathcal{S}(E_0, g)$.

При выполнении обеих предпосылок (а) и (б) вывод D является корректным выводом с целью g.

Доказательство. См. Приложение Б. □

Теперь мы можем показать, что правила L_o допускают корректные выводы.

Лемма 4.5. Пусть E — конечное нормализованное множество стандартных сообщений, а g — нормализованное стандартное сообщение. Если $g \in forge(E)$, то существует корректный вывод из E с целью g.

Доказательство. Положим $E_0 = E$ и $D = E_0 \to_{L_1} \cdots \to_{L_n} E_n$ — вывод цели g минимальной длины. Будем считать, что D удовлетворяет свойствам, сформулированным в лемме 4.3, пункт 2.

Покажем, что D удовлетворяет предпосылкам леммы 4.4, пунктов 1 и 2.

(1) Пусть $L_j \in L_d(s) \cap \mathcal{L}_d(t)$; тогда $t \in S(s)$. Для всех $i < j$ имеем $L_i \notin L_{oc}(s)$, поскольку правила из L_{oc} не создают стандартных термов, и $L_i \notin L_{oc}(s)$ по определению вывода (иначе t находился бы в левой части правила L_i). Следовательно, либо $s \in E_0$, либо существует $i < j$ такое, что $L_i \in \mathcal{L}_d(s)$. Если $L_j \in L_{od}(t)$ и t' — головной терм правила L_j, то, по определению декомпозиционных DH-правил, легко видеть, что $t \in \mathcal{S}(t')$. По лемме 4.3, 2 отсюда следует, что $t' \in E_0$ или существует t'-правило $L' \in D \cap L_d(t')$. Следовательно, по лемме 4.4, 1 имеем: если $L \in D \cap \mathcal{L}_d(t)$ для некоторого L и t, то $t \in \mathcal{S}(E_0)$.

(2) Пусть $L_i \in \mathcal{L}_c(t)$ и $i < n$. По минимальности вывода D найдётся $j > i$ такое, что t входит в левую часть правила L_j. Если $L_j \in L_d$, то, как и в пункте 1, получаем $t \in \mathcal{S}(E_0)$. Если $L_j \in L_c(t')$, то $t \in \mathcal{S}(t')$. Пусть теперь $L_j \in L_o(t')$. Сначала предположим, что t является головным термом L_j. По лемме 4.3, 2 существует t-правило $L' \in D \cap (L_d \cup L_c)$. Так как $L_i \in L_c(t)$ и, благодаря минимальности D, терм t может порождаться ровно одним правилом, имеем $L_i = L' \in L_c$; следовательно $t \neq Exp(\cdot, \cdot)$. Из определения DH-правил тогда следует $t \in \mathcal{S}(t')$. Пусть теперь t *не* является головным термом L_j. Если $t \notin \mathcal{S}(t')$, то существует терм t'' — головной терм L_j — такой, что $t \in \mathcal{S}(t'')$, и t'' имеет вид $Exp(\cdot, \cdot)$ (иначе t не мог бы исчезнуть из t'). По лемме 4.3, 2 либо $t'' \in E_0$, либо существует t''-правило $L' \in D \cap (L_d \cup L_c)$. Так как t'' имеет вид $Exp(\cdot, \cdot)$, получаем $L' \in D \cap L_d$. Из пункта 1 тогда следует $t'' \in \mathcal{S}(E_0)$, а значит $t \in \mathcal{S}(E_0)$. □

4.2 Правила Диффи–Хеллмана являются правилами оракула

Теперь мы докажем оставшиеся свойства, необходимые для оракульных правил, и тем самым покажем, что L_o действительно образует множество oracle rules (см. Предложение 4.7). Сначала нам понадобится лемма, аналогичная Лемме 3.6.

Лемма 4.6. Пусть $z_1, \ldots, z_n \in \mathbb{Z} \setminus \{0\}$, а $s, s_1, \ldots, s_n$ — нормализованные стандартные термы, удовлетворяющие условиям $s_i \neq s_j$ при $i \neq j$, $s_i \neq 1$ и $s_i \neq u$ для всех i, $s \neq u$, $u = \ulcorner Exp\big(s,\, s_1^{z_1} \cdots s_n^{z_n}\big) \urcorner, u = Exp(\,\cdot\,,\cdot\,)$. Пусть δ — замена $[\,u \to 2\,]$. Тогда $u = \ulcorner Exp\big(\ulcorner s\delta \urcorner,\, \ulcorner s_1\delta \urcorner^{z_1} \cdots \ulcorner s_n\delta \urcorner^{z_n}\big) \urcorner$.

Доказательство. См. Приложение Б. □

Теперь мы готовы сформулировать и доказать следующую теорему.

Предложение 4.7. Множество правил L_o является множеством *правил оракула.*

Доказательство. Проверим по очереди условия 1, 2 и 3 определения 2.11.

(1) Непосредственное следствие леммы 4.5.

(2) Утверждение вытекает из того, что ни один терм, созданный правилом из L_{oc}, не может быть декомпозирован с помощью правила из L_d.

(3) Пусть u — нормализованное стандартное сообщение, F — множество стандартных сообщений, причём $1 \in F$, и t — стандартное сообщение такое, что $F \cup \{u\} \;\to_{\mathcal{L}_c(u)}\; F, F \;\to_{L_o(t)}\; F, t$. Положим $\delta := [\,u \leftarrow 1\,]$. Если $u = t$, то $t\delta = 1 \in forge(F\delta)$, и требуемое выполнено. Предположим $u \neq t$. Из $F \to_{L_o(t)} F$ следует, что существуют $t', t_1, \ldots, t_n \in F$ и $z_1, \ldots, z_n \in \mathbb{Z} \setminus \{0\}$, такие что $t_i \neq t_j$ при $i \neq j$ и $t = \ulcorner Exp\big(t',\, t_1^{z_1} \cdots t_n^{z_n}\big) \urcorner$. Если $t' \neq Exp(\,\cdot\,,\cdot\,)$ или $u \neq t'$, то по лемме 3.6

$$\ulcorner t\delta \urcorner = \ulcorner Exp\big(\ulcorner t'\delta \urcorner,\, \ulcorner t_1^{\delta} \urcorner^{z_1} \ldots \ulcorner t_n^{\delta} \urcorner^{z_n}\big) \urcorner.$$

Таким образом, $t^\delta \in forge(F^\delta)$. Предположим теперь, что $u = t' = Exp(v, M)$. Тогда

$$\begin{aligned}
\ulcorner t^\delta \urcorner &= \ulcorner\ulcorner Exp\big(v, M_1^{z_1} \cdots t_n^{z_n}\big)\urcorner\delta\urcorner \\
&= \ulcorner Exp\big(v, M^\delta\, t_1^{\delta z_1} \cdots t_n^{\delta z_n}\big)\urcorner && (*) \\
&= \ulcorner Exp\big(v\delta, M^\delta (t_1\delta)^{z_1} \cdots (t_n\delta)^{z_n}\big)\urcorner && (**) \\
&= \ulcorner Exp\big(v, M\ulcorner t_1\delta\urcorner^{z_1} \cdots \ulcorner t_n\delta\urcorner^{z_n}\big)\urcorner && (***) \\
&= \ulcorner Exp\big(u, \ulcorner t_1\delta\urcorner^{z_1} \cdots \ulcorner t_n\delta\urcorner^{z_n}\big)\urcorner.
\end{aligned}$$

В переходе $(*)$ применяем лемму 3.4(2), используя, что $v \neq u$ и $u \neq t$. В $(**)$ снова используем условие $u \neq t$, а $(***)$ получаем, поскольку $u \notin S(v, M)$. Чтобы показать, что $\ulcorner t\delta\urcorner \in forge(\ulcorner F\delta\urcorner)$, достаточно убедиться, что $u \in forge(\ulcorner F\delta\urcorner)$. Из $F \setminus \{u\} \to_{\mathcal{L}_c(u)} F$ и $u = Exp(\cdot, \cdot)$ получаем $F\backslash u \to_{L_{oc}(u)} F$. Следовательно, существуют нормализованные термы $s, s_1, \ldots, s_n \in F \setminus \{u\}$ и целые $z_1', \ldots, z_n' \in \mathbb{Z}\setminus\{0\}$, такие что s и s_i удовлетворяют условиям леммы 4.6 и $u = \ulcorner Exp\big(s, s_1^{z_1} \cdots s_n^{z_n}\big)\urcorner$. Тогда по лемме 4.6 $u = \ulcorner Exp\big(\ulcorner s\delta\urcorner, \ulcorner s_1^{\delta\urcorner z_1} \cdots \ulcorner s_n^{\delta\urcorner z_n}\big)\urcorner$, и, следовательно, $u \in forge(F\delta)$. □

4.3 Принятие решения для правил DH

Следующее предложение показывает, что за полиномиальное время можно решить, выводится ли заданное сообщение из конечного множества сообщений при *одном* применении правила оракула.

Предложение 4.8. Для нарушителя DH задача OracleRule разрешима в детермированное полиномиальное время.

Доказательство. Нужно построить детермированный алгоритм полиномиального времени, который по данным E и t решает, существуют ли $t', t_1, \ldots, t_n \in E$ и $z_1, \ldots, z_n \in \mathbb{Z}$ такие, что $t = \ulcorner Exp\big(t', t_1^{z_1} \cdots t_n^{z_n}\big)\urcorner$. Нетрудно убедиться, что $E \to_{L_o} E, t$ точно тогда, когда выполняется одно из условий:

а) $t \neq Exp(\,\cdot, \cdot\,)$ и
   1) $t \in E$, или
   2) существует M такое, что $Exp(t, M) \in E$ и $\mathcal{F}(M) \subseteq E$;

б) $t = Exp(v, M)$ и
   1) $v \in E$ и $\mathcal{F}(M) \subseteq E$, или

2) существует M' такое, что $Exp(v, M') \in E$ и $E' := \{ t' \mid$ мультипликативные показатели t' в M и M'различаются$\} \subseteq E$.

Исходя из этой характеристики, легко вывести полиномиальный алгоритм для решения задачи $E \to_{L_o} E, t$. □

Немедленным следствием предложения 4.8, а также предложения 4.7 и теоремы 3.2 является:

Следствие 4.9. Для нарушителя DH задача Derive решается в детерминированное полиномиальное время.

5 Правила DH допускают атаки с полиномиальным произведением показателей

В этом разделе мы показываем, что задача Insecure NP-полна для нарушителя DH (см. Теорему 5.23). В силу Теоремы 3.1, Предложения 4.7 и Предложения 4.8 остаётся показать, что правила DH действительно допускают атаки с полиномиально ограниченным произведением показателей. Для этого мы свяжем с минимальной атакой (π, σ) подстановку σ^2 и линейную систему уравнений, обладающую двумя свойствами:

(i) σ^Z совпадает с σ, за исключением того, что все показатели произведения в σ заменены новыми целочисленными переменными;

(ii) (π, σ') остаётся атакой для каждой подстановки σ', получаемой из σ^Z подстановкой значений переменных, удовлетворяющих линейной системе.

Размер этой системы можно ограничить полиномом от размера протокола, а значит и размер её решений тоже ограничивается полиномиально (см. [23]). Тем самым мы получаем атаку с полиномиально ограниченными произведениями показателей (см. Предложение 5.22).

В следующем подразделе мы формально определим сообщения, в которых показатели могут быть линейными выражениями. Перед тем как перейти к подробному изложению, в § 5.2 мы дадим интуитивное объяснение доказательства Предложения 5.22. Полное доказательство приведено в 5.3–5.7.

5.1 Открытые сообщения и системы уравнений

В этом разделе мы вводим открытые сообщения и произведения, отображения оценки, системы уравнений, а также различные меры их размера.

Определение 5.1. Пусть Z — множество переменных. Обозначим через $\mathcal{M} = \mathcal{M}(Z)$ множество *открытых сообщений* над Z, через $\mathcal{P} = \mathcal{P}(Z)$ — множество *открытых произведений* над Z, а через $\mathcal{L}_{\exp} = \mathcal{L}_{\exp}(Z)$ — множество *линейных выражений* над Z. Эти множества задаются следующей грамматикой:

$$\begin{aligned} \mathcal{M} &::= A \mid \langle \mathcal{M}, \mathcal{M} \rangle \mid \{\mathcal{M}\}^s_{\mathcal{M}} \mid \{\mathcal{M}\}^p_K \mid Exp(\mathcal{M}, \mathcal{P}), \\ \mathcal{P} &::= \mathcal{M}^{\mathcal{L}_{\exp}} \mid \mathcal{M}^{\mathcal{L}_{\exp}} \cdot \mathcal{P}, \\ \mathcal{L}_{\exp} &::= \mathbb{Z} \mid Z \mid \mathcal{L}_{\exp} + \mathcal{L}_{\exp} \mid \mathbb{Z} \cdot \mathcal{L}_{\exp}. \end{aligned}$$

Размер $|e|$ линейного выражения e — это число символов, необходимых для записи e (целые кодируются двоично). Говорим, что e и e' *равны*, если они эквивалентны по ассоциативности и коммутативности сложения (сокращённо AC_+). Для множества линейных выражений S и выражения e мы говорим, что e принадлежит S, если класс эквивалентности по модулю $\mathrm{AC}_+(e)$ для e является одним из классов эквивалентности классов, индуцированных по S. Тогда $e \in S$ означает, что $\mathrm{AC}_+(e)$ совпадает с одним из классов, индуцированных S. Отношение включения между наборами линейных выражений определяется аналогично.

Для открытого сообщения или произведения t обозначим через $\mathcal{L}_{\mathrm{exp}}(t)$ множество линейных выражений, встречающихся в t. Пусть $\mathcal{S}(t)$ — множество подтермов t, а $|t| = \mathrm{Card}(\mathcal{S}(t))$ — их количество. Следуя принятой ранее нотации, положим

$$S_{\mathrm{ext}}(t) = \mathcal{S}(t) \cup \{\, M \mid \mathrm{Exp}(u, M) \in \mathcal{S}(t)\}, \qquad |t|_{\mathrm{ext}} = \mathrm{Card}(\mathcal{S}_{\mathrm{ext}}(t)).$$

Также определим $|t|_{\mathrm{exp}} = 0$, если t не является произведением, и $|t|_{\mathrm{exp}} = |e_1| + \cdots + |e_n|$, если $t = e_1^1 \ldots e_n^n$. Для конечного множества открытых сообщений или произведений E обозначим $|E|_{\mathrm{exp}} = \sum_{s \in E} |s|_{\mathrm{exp}}$. Наконец,

$$\|t\|_{\mathrm{exp}} = |S(t)|_{\mathrm{exp}}, \qquad \|t\| = |t| + \|t\|_{\mathrm{exp}}, \qquad \|t\|_{\mathrm{ext}} = |t|_{\mathrm{ext}} + \|t\|_{\mathrm{exp}}.$$

Лемма 5.2. Для любого открытого сообщения или произведения t выполняется

$$|t|_{\mathrm{ext}} \;\leq\; 2 \cdot |t|, \qquad \text{и, следовательно,} \qquad \|t\|_{\mathrm{ext}} \;\leq\; 2 \cdot \|t\|.$$

Заметим, что определения $|\cdot|$, $\|\cdot\|_{\mathrm{exp}}$ и $\|\cdot\|$ для открытых сообщений и произведений совпадают с соответствующими определениями для (закрытых) сообщений.

Приведённые выше определения и меры для открытых сообщений и произведений естественным образом переносятся на множества открытых сообщений, открытых произведений и т. д.

Назовём отображение $\beta : Z \to \mathbb{Z}$ *отображением оценки*. Значение $\beta(e) \in \mathbb{Z}$ линейного выражения e определяется обычным образом. Очевидно, β естественным образом распространяется на открытые сообщения, открытые произведения, а также на их множества.

В дальнейшем в этом подразделе β всегда фиксируется как отображение оценки из Z в $\mathbb{Z}$.

Линейной системой уравнений $\mathcal{E}$ (над Z) называется конечное множество равенств вида $e = e'$, где e и e' — линейные выражения над Z. Её *размер* $|\mathcal{E}| = \sum_{e=e' \in \mathcal{E}} \big(|e| + |e'|\big)$. Отображение оценки β является *решением* системы (обозначаем $\beta \models \mathcal{E}$), если $\beta(e) = \beta(e')$ для каждого уравнения $e = e' \in \mathcal{E}$. $L_{\exp}(\mathcal{E}) = \big\{\, e \mid e = e' \text{ или } e' = e \in \mathcal{E} \big\}$. Положим $R_{\mathcal{E}} = \big\{\, (e, e') \mid e = e' \in \mathcal{E} \big\} \subseteq \mathcal{L}_{\exp}(\mathcal{E}) \times \mathcal{L}_{\exp}(\mathcal{E})$, $\quad R^*_{\mathcal{E}}$ — рефлексивно-транзитивное замыкание $R_{\mathcal{E}}$. Пишем $\mathcal{E} \cong \mathcal{E}'$, если $R^*_{\mathcal{E}} = R^*_{\mathcal{E}'}$, и $\mathcal{E} \subseteq \mathcal{E}'$, если $R^*_{\mathcal{E}} \subseteq R^*_{\mathcal{E}'}$. Таким образом, линейные уравнения рассматриваются с точностью до рефлексивности и транзитивности равенства. Напомним также, что линейные выражения эквивалентны по правилу AC_+.

5.2 Обзор доказательства Предложения 5.22

Ниже приведён неформальный «вид сверху» на доказательство Предложения 5.22, позволяющего полиномиально ограничить величины показателей произведения в атаках.

Ключевым элементом является Лемма 5.21, в которой говорится следующее. Пусть $t, t_1, \ldots, t_n$ — открытые сообщения и β — отображение оценки, такое что $\ulcorner \beta(t) \urcorner \in \mathrm{forge}\big(\ulcorner \beta(t_1) \urcorner, \ldots, \ulcorner \beta(t_n) \urcorner\big)$. Тогда существует расширение β (обозначаем его тем же символом) и система линейных уравнений $\mathcal{E}$, удовлетворяющие

(1) $\beta \models \mathcal{E}$;

(2) для всякого $\beta' \models \mathcal{E}$

$$\ulcorner \beta'(t) \urcorner \in \mathrm{forge}\big(\ulcorner \beta'(t_1) \urcorner, \ldots, \ulcorner \beta'(t_n) \urcorner\big);$$

(3) размер $\mathcal{E}$ ограничен полиномом от $\|t_1, \ldots, t_n, t\|_{\mathrm{ext}}$.

Доказательство этой леммы довольно громоздко. Основная идея состоит в том, чтобы заменить сообщения в выводе D от $\ulcorner\beta(t_1)\urcorner, \ldots, \ulcorner\beta(t_n)\urcorner$ к $\ulcorner\beta(t)\urcorner$ на *открытые* сообщения, совпадающие с исходными, за исключением показателей степеней произведения. Более точно, каждое t_i заменяется на открытое сообщение t'_i, которое мы называем β-нормальной формой (или β-термом) и для которого $\beta(t'_i) = \ulcorner\beta(t_i)\urcorner$. Иными словами, t'_i служит символическим представлением нормальной формы $\beta(t_i)$. После этого можно имитировать вывод D в (символическом) выводе D', начинающемся с β-нормальных форм $t'_1, \ldots, t'_n$. Промежуточные термы, возникающие в D', также являются β-нормальными формами соответствующих термов из D. Система линейных уравнений $\mathcal{E}$ постепенно эволюционирует по мере замены t_i на их β-нормальные формы и симуляции вывода D.

Более формально, преобразуя t_i в β-нормальную форму, мы одновременно «прикрепляем» к этой нормальной форме систему уравнений. То есть вводим то, что будем называть β-*кортежем* $(t'_i, \mathcal{E}_i)$, где t'_i — β-нормальная форма терма t_i, а $\mathcal{E}_i$ — такая система линейных уравнений, что $\beta \models \mathcal{E}_i$ и для любой оценки β', удовлетворяющей $\mathcal{E}_i$, выполняется $\ulcorner\beta'(t_i)\urcorner = \ulcorner\beta'(t'_i)\urcorner$.

Иными словами, t'_i служит символическим представлением нормальной формы не только для $\beta(t_i)$, но и для $\beta'(t_i)$ при всех $\beta' \models \mathcal{E}_i$ (в последнем случае t'_i возможно требуется дополнительно нормализовать, чтобы совпасть с $\ulcorner\beta'(t_i)\urcorner$). Итоговая система уравнений $\mathcal{E}$ получается как объединение систем из β-кортежей для $t_1, \ldots, t_n, t$ и уравнений, возникающих в процессе симуляции вывода D.

Очевидно, чтобы доказать лемму, необходимо ограничить размер β-кортежей, то есть β-нормальных форм (β-термов) вместе с присоединившимися к ним системами уравнений, а также размер уравнений, возникающих при симуляции вывода D (подробности см. в последующих подразделах).

Опираясь на сформулированную выше лемму, нетрудно доказать Предложение 5.22, утверждающее, что для каждой минимальной атаки (π, σ) существует атака (π, σ') той же структуры (то есть σ и σ' совпадают с точностью до показателей степеней произведений), причём полный размер σ' и её показатели можно ограничить полиномом от размера протокола.

Суть доказательства Предложения 5.22 такова. К подстановке σ приписывается символическая версия σ^Z, в которой все показатели заменены новыми целыми переменными. Далее вышеупомянутая лемма применяется к случаю $t = R_i\sigma^Z$ и $t_j = S_j\sigma^Z$ для всех $j \in \{0, \ldots, i-1\}$. Для каждого i лемма даёт систему уравнений $\mathcal{E}_i$, и любое решение β' объединённой системы $\bigcup_i \mathcal{E}_i$ порождает новую атаку $(\pi, \beta'(\sigma^Z))$ на протокол. Поскольку объединённая система уравнений «небольшая», а линейные системы имеют «небольшие» решения β' (см. [23]), получаем атаку (π, σ'), где $\sigma' = \beta'(\sigma^Z)$, с полиномиально ограниченными показателями.

В следующем подразделе мы вводим β-кортежи. Затем показываем, что такие кортежи существуют (раздел 5.4). В 5.5–5.6 оцениваем размеры β-термов и соответствующих им систем уравнений, а следовательно, и размер β-кортежей в целом. Наконец, в § 5.7 доказываем упомянутые Лемму 5.21 и Предложение 5.22 и, опираясь на них, выводим, что задача Insecure NP-полна для нарушителя DH.

5.3 β-эквивалентность, β-кортежи и $\approx_\beta$-системы уравнений

Определение 5.3. Пусть заданы отображение оценки β и два открытых сообщения (или открытых произведений) t и t'. Говорим, что t и t' *β-равны* (обозначаем $t =_\beta t'$), если $\beta(t) = \beta(t')$.[1] Называем t и t' *β-эквивалентными* (пишем $t \approx_\beta t'$), если $\ulcorner\beta(t)\urcorner = \ulcorner\beta(t')\urcorner$.

Определение 5.4. Пусть $t =_\beta t'$. Система линейных уравнений $\mathcal{E}$ называется *$=_\beta$-системой уравнений* для t и t', если выполняются оба условия

(1) $\beta \models \mathcal{E}$;

(2) $t \approx_{\beta'} t'$ для всякого $\beta' \models \mathcal{E}$.

Мы теперь показываем, что «небольшие» $=_\beta$-системы уравнений действительно существуют. Напомним, что, например, запись $\|t, t'\|_{\text{ext}}$ означает $\|\{t, t'\}\|_{\text{ext}}$.

Лемма 5.5. Пусть заданы отображение оценки β и открытые сообщения (или открытые произведения) t и t', причём $t =_\beta t'$. Тогда существует $=_\beta$-система уравнений $\mathcal{E}^{=_\beta}_{t,t'}$ размера не более $2\|t, t'\|^3_{\text{ext}}$, соответствующая t и t'.

[1] Равенство понимается по модулю ассоциативности и коммутативности умножения в произведении.

Доказательство. Определим

$$R \subseteq S_{\text{ext}}(t,t') \times S_{\text{ext}}(t,t')$$

так, чтобы для каждой пары $(s,s') \in R$ выполнялось $s =_\beta s'$. Точнее, R — наименьшее бинарное отношение на $S_{\text{ext}}(t,t')$, удовлетворяющее условиям

— $(t,t') \in R$;

— Если $(s,s') \in R$ и, по построению, $s =_\beta s'$, причём $s = \langle t_1, t_2 \rangle$, то найдутся открытые сообщения t_1', t_2' такие, что $s' = \langle t_1', t_2' \rangle$. Тогда $\langle t_1, t_1' \rangle \in R$ и $\langle t_2, t_2' \rangle \in R$. Для случаев шифрования вводятся аналогичные условия на R.

— Если $(s,s') \in R$ и s — произведение $t_1^{e_1} \cdots t_n^{e_n},\ n \geq 1$, то s' также является произведением $t_1'^{e_1'} \cdots t_n'^{e_n'},\ n \geq 1$. Если для некоторых i,j выполнено $t_i =_\beta t_j'$, то пара $\langle t_i, t_j' \rangle$ принадлежит R. Заметим, что из равенства $s =_\beta s'$ следует: для каждого t_i существует хотя бы один $=_\beta$-равный ему терм t_j'.

— Если $t = Exp(u,M)$ для некоторого открытого сообщения u и открытого произведения M, то $t' = Exp(u',M')$ для некоторого открытого сообщения u' и открытого произведения M'. Тогда $(u,u') \in R$ и $(M,M') \in R$.

Для каждой пары $(s,s') \in R$ определим систему уравнений $\mathcal{E}_{(s,s')}$ следующим образом. Если s (а значит и s') не является произведением, то $\mathcal{E}_{(s,s')}$ — пустое множество. Иначе s имеет вид $t_1^{e_1} \cdots t_n^{e_n},\ n \geq 1$, а s' — вид $t_1'^{e_1} \cdots t_n'^{e_n}$. Положим $\mathcal{E}_{(s,s')} = \left\{ e_i = e_j' \;\middle|\; (t_i, t_j') \in R \right\}$.

Структурной индукцией нетрудно показать, что $\mathcal{E}_R = \bigcup_{(s,s') \in R} \mathcal{E}_{(s,s')}$ является $=_\beta$-системой уравнений для t и t'. Очевидно, её размер не превосходит $2\|t,t'\|_{\text{ext}}^3$. □

В дальнейшем мы будем обозначать $\mathcal{E}_{t,t'}^{=_\beta}$, построенную в доказательстве, как *$=_\beta$-систему уравнений, индуцированную парой t и t'.*

Замечание 5.6 Система $\mathcal{E}_{t,t'}^{=_\beta}$, сконструированная в Лемме 5.5, определена однозначно.

Нам также потребуется приписывать $\approx_\beta$-эквивалентным термам систему уравнений, которую мы называем *$\approx_\beta$-системой уравнений.*

Определение 5.7 Пусть заданы β и открытые сообщения (или произведения) t и t' такие, что $t \approx_\beta t'$. Говорим, что $\mathcal{E}$ является *$\approx_\beta$-системой уравнений* для t и t', если

а) $\beta \models \mathcal{E}$, и

б) $t \approx_{\beta'} t'$ для всякой $\beta' \models \mathcal{E}$.

Чтобы построить такую систему уравнений для пары t и t', введём понятие β-кортежа.

Определение 5.8. Пусть задано отображение оценки β и открытое сообщение (или открытое произведение) t. Пара $(t', \mathcal{E})$, где t' — открытое сообщение (или произведение), а $\mathcal{E}$ — система линейных уравнений, называется *β-кортежем* для t, если выполняются условия

(1) $\beta(t') = \ulcorner\beta(t)\urcorner$;

(2) $\beta \models \mathcal{E}$;

(3) $t \approx_{\beta'} t'$ для всякой $\beta' \models \mathcal{E}$.

терм t' называют *β-термом* (или *β-нормальной формой*) терма t, а $\mathcal{E}$ — *β-системой уравнений* для t.

Следующая лемма показывает, как $\approx_\beta$-систему уравнений можно получить из β-кортежей.

Лемма 5.9. Пусть t и t' — открытые сообщения или произведения такие, что $t \approx_\beta t'$. Предположим, что для t задан β-кортеж $(s, \mathcal{E})$, а для t' — β-кортеж $(s', \mathcal{E}')$. Пусть $\mathcal{E}^{=_\beta}_{s,s'}$ — какая-нибудь $=_\beta$-система уравнений для s и s' (такая система всегда существует). Тогда

$$\mathcal{E}^{\approx_\beta}_{t,t'} \;=\; \mathcal{E} \;\cup\; \mathcal{E}' \;\cup\; \mathcal{E}^{=_\beta}_{s,s'}$$

является $\approx_\beta$-системой уравнений для t и t'.

Доказательство. Сначала покажем, что для s и s' всегда существует $=_\beta$-система уравнений. Поскольку $\beta(s) = \ulcorner\beta(t)\urcorner = \ulcorner\beta(t')\urcorner = \beta(s')$, имеем $s =_\beta s'$, а по лемме 5.5 существует $=_\beta$-система, которую обозначим $\mathcal{E}^{=_\beta}_{s,s'}$.

Теперь докажем, что $\mathcal{E}^{\approx_\beta}_{t,t'} = \mathcal{E} \cup \mathcal{E}' \cup \mathcal{E}^{=_\beta}_{s,s'}$ является $\approx_\beta$-системой для t и t'. Очевидно, $\beta \models \mathcal{E}^{\approx_\beta}_{t,t'}$. Пусть $\beta' \models \mathcal{E}^{\approx_\beta}_{t,t'}$; нужно показать, что $\ulcorner\beta'(t)\urcorner = \ulcorner\beta'(t')\urcorner$.

Из $\beta' \models \mathcal{E}, \mathcal{E}'$ получаем $\beta'(s) = \beta'(t)$ и $\beta'(s') = \beta'(t')$, а из $\beta' \models \mathcal{E}^{=_\beta}_{s,s'}$ следует $\beta'(s) = \beta'(s')$. Следовательно, $\ulcorner\beta'(t)\urcorner = \ulcorner\beta'(s)\urcorner = \ulcorner\beta'(s')\urcorner = \ulcorner\beta'(t')\urcorner$, что и требовалось. □

5.4 Существование β-кортежей

Покажем, что для любого открытого сообщения или произведения существует β-кортеж.

Лемма 5.10. Пусть t — открытое сообщение или открытое произведение, а β — отображение оценки. Тогда для t существует β-кортеж.

Доказательство. Построим пару $(t^\beta, \mathcal{E}_t^\beta)$ индукцией по t.

— Если $t \in \mathcal{A}$, то полагаем $t^\beta = t$, $\mathcal{E}_t^\beta = \varnothing$. Очевидно, $(t^\beta, \mathcal{E}_t^\beta)$ — β-кортеж для t.

— Пусть $t = \langle t_1, t_2 \rangle$. По индукционному предположению имеем $(t_1^\beta, \mathcal{E}_1^\beta)$ и $(t_2^\beta, \mathcal{E}_2^\beta)$ — β-кортежи для t_1 и t_2. Определяем $t^\beta = \langle t_1^\beta, t_2^\beta \rangle$, $\mathcal{E}_t^\beta = \mathcal{E}_1^\beta \cup \mathcal{E}_2^\beta$. Аналогично строятся β-кортежи для случая шифрования. Индукцией легко проверить, что $(t^\beta, \mathcal{E}_t^\beta)$ действительно является β-кортежем для t.

— Пусть $t = t_1^{e_1} \cdots t_n^{e_n}$. Для каждого i возьмём β-кортеж $(t_i^\beta, \mathcal{E}_{t_i}^\beta)$. Разобьём $\{t_1, \ldots, t_n\}$ на классы эквивалентности $C_1, \ldots, C_l$ по $\approx_\beta$; положим $e_{C_j} = \sum_{t_i \in C_j} e_i$ и выберем представителя $s_{C_j} \in C_j$, причём без ограничения общности считаем, что для всех $s \in C_1$ выполняется $s \approx_\beta 1$ (класс C_1 может быть пустым). Индукционное предположение даёт $s^\beta = 1$ для каждого $s \in C_1$, так как $\beta(s^\beta) = \ulcorner \beta(s) \urcorner = 1$. Обозначим $J = \{\, j \in \{2, \ldots, l\} \mid \beta(e_{C_j}) = 0\}$; если $C = \{s_1, \ldots, s_k\}$ — класс, элементы которого попарно $\approx_\beta$-эквивалентны, а s_j^β — β-терм для s_j, то кладём $\mathcal{E}_C^\beta = \bigcup_{i \neq j} \mathcal{E}^{=_\beta}_{s_i^\beta, s_j^\beta}$. Если $C = \{s_1, \ldots, s_k\}$ — класс, элементы которого попарно $\approx_\beta$-эквивалентны, и s_j^β — β-терм для s_j, положим

$$\mathcal{E}_C^\beta = \bigcup_{i \neq j} \mathcal{E}^{=_\beta}_{s_i^\beta, s_j^\beta}.$$

Заметим, что $\beta(s_i^\beta) = \ulcorner \beta(s_i) \urcorner = \ulcorner \beta(s_j) \urcorner = \beta(s_j^\beta)$, следовательно $s_i^\beta =_\beta s_j^\beta$, и по лемме 5.5 существует $=_\beta$-система $\mathcal{E}^{=_\beta}_{s_i^\beta, s_j^\beta}$. Положим

$$t^\beta = \begin{cases} 1, & \text{если } J = \{2, \ldots, l\}, \\ \displaystyle\prod_{j \notin J \cup \{1\}} (s_{C_j}^\beta)^{e_{C_j}}, & \text{иначе.} \end{cases}$$

Далее положим

$$\mathcal{E}^\beta = \bigcup_{i=1}^{n} \mathcal{E}_{t_i}^\beta \cup \bigcup_{j=2}^{l} \mathcal{E}_{C_j}^\beta \cup \bigcup_{j \in J} \{\, e_{C_j} = 0\}.$$

Индукцией легко показать, что $(t^\beta, \mathcal{E}^\beta)$ — β-кортеж для t: действительно, из индукционного предположения следует $\beta \models \mathcal{E}^\beta$. По определению функции нормализации нетрудно проверить, что, если $J = \{2, \ldots, l\}$, то $\ulcorner \beta(t) \urcorner = 1$, а значит $t^\beta = \ulcorner \beta(t) \urcorner$. В противном случае

$$\mathcal{E}_t^\beta = \bigcup_{i=1}^{n} \mathcal{E}_{t_i}^\beta \cup \bigcup_{j=2}^{l} \mathcal{E}_{C_j}^\beta \cup \bigcup_{j \in J} \{ e_{C_j} = 0 \}.$$

Индукционное предположение даёт, что $(t^\beta, \mathcal{E}_t^\beta)$ является β-кортежем для t: действительно, индукция обеспечивает $\beta \models \mathcal{E}_t^\beta$; по определению функции нормализации нетрудно проверить, что при $J = \{2, \ldots, l\}$ имеем $\ulcorner \beta(t) \urcorner = 1$, а значит $t^\beta = \ulcorner \beta(t) \urcorner$, тогда как при $J \neq \{2, \ldots, l\}$ выполняется $\ulcorner \beta(t) \urcorner = \prod_{j \notin J \cup \{1\}} \ulcorner \beta(s_{C_j}) \urcorner^{\beta(e_{C_j})}$, и, поскольку по индукции $\beta(s_{C_j}^\beta) = \ulcorner \beta(s_{C_j}) \urcorner$, получаем $\beta(t^\beta) = \ulcorner \beta(t) \urcorner$; следовательно, $\beta(t^\beta) = \ulcorner \beta(t) \urcorner$. Пусть теперь $\beta' \models \mathcal{E}_t^\beta$; если $s, s' \in C_j$ и $s \neq s'$.По определению $\mathcal{E}_t^\beta$ имеем $\beta' \models \mathcal{E}_t^\beta \cup \mathcal{E}_s^\beta \cup \mathcal{E}_{s_i^\beta, s_j^\beta}^{=\beta}$ $(= \mathcal{E}_{s_i^\beta, s_j^\beta}^{\approx\beta})$. Следовательно, по лемме 5.9 $\ulcorner \beta'(s) \urcorner = \ulcorner \beta'(s') \urcorner$. Поскольку $s^\beta = 1$, получаем $\beta'(s^\beta) = 1$ для каждого $s \in C_1$; кроме того, для $j \in J$ имеем $\beta'(e_{C_j}) = 0$. Отсюда непосредственно следует $\ulcorner \beta'(t) \urcorner = \ulcorner \beta'(t^\beta) \urcorner$.

— Если $t = \mathrm{Exp}(u, M)$ и при этом $\beta(u) \neq \mathrm{Exp}(\,\cdot, \cdot\,)$, то по индукционному предположению существуют β-кортежи $(u^\beta, \mathcal{E}_u^\beta)$ для u и $(M^\beta, \mathcal{E}_M^\beta)$ для M. Положим

$$t^\beta = \begin{cases} u^\beta, & \text{если } \beta(M) = 1, \\ \mathrm{Exp}\big(u^\beta, M^\beta\big), & \text{иначе,} \end{cases}$$

В обоих случаях мы присваиваем:

$$\mathcal{E}_t^\beta = \mathcal{E}_u^\beta \cup \mathcal{E}_M^\beta.$$

Окончим доказательство, показав, что $(t^\beta, \mathcal{E}_t^\beta)$ действительно является β-кортежем для t. Очевидно, $\beta \models \mathcal{E}_t^\beta$, поэтому осталось убедиться, что

$$\ulcorner \beta(t^\beta) \urcorner = \ulcorner \beta(t) \urcorner \quad \text{и} \quad \ulcorner \beta'(t^\beta) \urcorner = \ulcorner \beta'(t) \urcorner \text{ для всякого } \beta' \models \mathcal{E}_t^\beta.$$

Возникают два случая.

(1) $\ulcorner\beta(M)\urcorner = 1$. Тогда $\ulcorner\beta(t)\urcorner = \ulcorner\beta(u)\urcorner$. По индукции $\ulcorner\beta(t)\urcorner = \ulcorner\beta(u)\urcorner = \ulcorner\beta(u^\beta)\urcorner = \ulcorner\beta(t^\beta)\urcorner$. Кроме того, $\beta(M^\beta) = \ulcorner\beta(M)\urcorner = 1$, откуда $M^\beta = 1$ и, по индукции, $\ulcorner\beta'(M^\beta)\urcorner = \ulcorner\beta'(M)\urcorner = 1$. Следовательно,

$$\ulcorner\beta'(t)\urcorner \overset{(*)}{=} \ulcorner\beta'(u)\urcorner \overset{(**)}{=} \ulcorner\beta'(u^\beta)\urcorner = \ulcorner\beta'(t^\beta)\urcorner,$$

где $(*)$ следует из индукционного предположения и определения $\mathcal{E}_t^\beta$, а $(**)$ — из определения t^β.

(2) Или $\ulcorner\beta(M)\urcorner \neq 1$. Тогда

$$\ulcorner\beta(t)\urcorner \;=\; \mathrm{Exp}\big(\ulcorner\beta(u)\urcorner, \ulcorner\beta(M)\urcorner\big) \overset{(*)}{=} \mathrm{Exp}\big(\ulcorner\beta(u^\beta)\urcorner, \beta(M^\beta)\big) \overset{(**)}{=} \ulcorner\beta(t^\beta)\urcorner,$$

где $(*)$ получено по индукции и определению $\mathcal{E}_t^\beta$, а $(**)$ — по определению t^β.

Пусть теперь $\beta' \models \mathcal{E}_t^\beta$. Тогда

$$\ulcorner\beta'(t)\urcorner \;=\; \mathrm{Exp}\big(\ulcorner\beta'(u)\urcorner, \ulcorner\beta'(M)\urcorner\big) \overset{(*)}{=} \mathrm{Exp}\big(\ulcorner\beta'(u^\beta)\urcorner, \ulcorner\beta'(M^\beta)\urcorner\big) \overset{(**)}{=} \ulcorner\beta'(t^\beta)\urcorner,$$

где $(*)$ снова следует из индукции и определения $\mathcal{E}_t^\beta$, а $(**)$ — из определения t^β.

— Если $t = \mathrm{Exp}(u, M)$ и $\ulcorner\beta(u)\urcorner = \mathrm{Exp}(u', M')$, то по индукции существует β-кортеж $\big(u^\beta, \mathcal{E}_u^\beta\big)$ для u. В частности, $\beta(u^\beta) = \ulcorner\beta(u)\urcorner$, так что u^β имеет вид $\mathrm{Exp}(u'', M'')$, где $\beta(u'') = u'$ и $\beta(M'') = M'$. Кроме того, по индукции существует β-кортеж $\big((M''\cdot M)^\beta, \mathcal{E}^\beta_{(M''\cdot M)}\big)$ для $(M''\cdot M)$. Положим

$$t^\beta = \begin{cases} u'', & \text{если } \ulcorner\beta(M''\cdot M)\urcorner = 1, \text{ т. е. } \ulcorner M'\cdot\beta(M)\urcorner = 1, \\ \mathrm{Exp}\big(u'', (M''\cdot M)^\beta\big), & \text{иначе,} \end{cases}$$

В обоих случаях устанавливаем, что:

$$\mathcal{E}_t^\beta = \mathcal{E}_u^\beta \cup \mathcal{E}^\beta_{(M''\cdot M)}.$$

Индукцией теперь можно показать, что $(t^\beta, \mathcal{E}_t^\beta)$ действительно является β-кортежем для t. Очевидно, $\beta \models \mathcal{E}_t^\beta$. Следовательно, остаётся доказать равенства $\beta(t^\beta) = \ulcorner\beta(t)\urcorner$ и $\ulcorner\beta'(t)\urcorner = \ulcorner\beta'(t^\beta)\urcorner$ для всякого $\beta' \models \mathcal{E}_t^\beta$. Сначала положим $(u^\beta, \mathcal{E}_u^\beta) = \mathrm{Exp}(u'', M'')$, как было выше. Мы знаем, что $\ulcorner\beta(t)\urcorner = \ulcorner\mathrm{Exp}\big(\beta(u), \beta(M)\big)\urcorner = \ulcorner\mathrm{Exp}\big(u', \ulcorner M'\cdot\beta(M)\urcorner\big)\urcorner$. Если $\ulcorner M'\cdot\beta(M)\urcorner = 1$, то $\ulcorner\beta(t)\urcorner = u' = \beta(u'') = \beta(t^\beta)$. Иначе

$$\begin{aligned}\ulcorner\beta(t)\urcorner = Exp\big(u', \ulcorner M'\cdot\beta(M)\urcorner\big) &= \mathrm{Exp}\big(\beta(u''), \ulcorner\beta(M'')\cdot\beta(M)\urcorner\big)\\ = \mathrm{Exp}\big(\beta(u''), \ulcorner\beta\big(M''\cdot M\big)\urcorner\big) &\overset{(*)}{=} \mathrm{Exp}\big(\beta(u''), \beta\big((M''\cdot M)^\beta\big)\big) \ (**) \overset{(**)}{=} \beta(t^\beta),\end{aligned}$$

где равенство $(*)$ получено по индукции, а $(**)$ — по определению t^β. Пусть теперь $\beta'(t) \models \mathcal{E}_t^\beta$. Тогда $\ulcorner\beta'(t)\urcorner = \ulcorner Exp\big(\beta'(u), \beta'(M)\big)\urcorner$. Поскольку $\beta' \models \mathcal{E}_u^\beta$, из индукционного предположения следует $\ulcorner\beta'(u)\urcorner = \ulcorner\beta'(u^\beta)\urcorner = \ulcorner\beta'\big(\mathrm{Exp}(u'', M'')\big)\urcorner$. Отсюда $\ulcorner\beta'(t)\urcorner = \ulcorner\mathrm{Exp}\big(\beta'(u^\beta), \beta'(M)\big)\urcorner = \ulcorner\mathrm{Exp}\big(\beta'(u''), \beta'(M'')\cdot\beta'(M)\big)\urcorner = \ulcorner\mathrm{Exp}\big(\beta'(u''), \beta'(M''\cdot M)\big)\urcorner$. Так как $\beta' \models \mathcal{E}^\beta_{(M''\cdot M)}$, по индукции имеем $\ulcorner\beta'\big((M''\cdot M)^\beta\big)\urcorner = \ulcorner\beta'(M''\cdot M)\urcorner$. Следовательно, $\ulcorner\beta'(t)\urcorner = \ulcorner\mathrm{Exp}\big(\beta'(u''), \beta'\big((M''\cdot M)^\beta\big)\big)\urcorner$. Если $t^\beta = \mathrm{Exp}\big(u'', (M''\cdot M)^\beta\big)$, то $\ulcorner\beta'(t)\urcorner = \ulcorner\beta'(t^\beta)\urcorner$. В противном случае $t^\beta = u''$ и $\ulcorner\beta(m''\cdot M)\urcorner = 1$, а значит $(M''\cdot M)^\beta = 1$, и снова $\beta'(t) = \beta'(t^\beta)$. Таким образом, $\ulcorner\beta'(t)\urcorner = \ulcorner\beta'(t^\beta)\urcorner$. □

5.5 Ограничение размера β-термов

Начиная с этого места, через t^β мы будем обозначать β-терм сообщения (или произведения) t, построенный в доказательстве леммы 5.10. Наша цель — показать, что всегда существует β-кортеж для t, размер которого ограничен полиномом от $\|t\|$. Доказательство разбивается на два шага: в настоящем подразделе мы получаем оценку размера t^β, а в следующем — оцениваем размер системы уравнений, ассоциированной с t^β.

Для начала установим, что β-терм определяется однозначно.

Лемма 5.11. Для любого открытого сообщения или произведения t, такого что $\beta(t) = \ulcorner\beta(t)\urcorner$, выполнено $t^\beta = t$.

Доказательство. См. Приложение B. □

Для множества E открытых сообщений или произведений положим

$$E^\beta = \{\, t^\beta \mid t \in E\}.$$

В следующей лемме мы получим верхнюю границу для $|t^\beta|_{\text{ext}}$, а в Лемме 5.14 — для $\|t^\beta\|_{\exp}$. Объединив эти результаты, Лемма 5.15 даёт оценку для $\|t^\beta\|_{\text{ext}}$.

Лемма 5.12. Пусть $t, t_1, \ldots, t_n$ — открытые сообщения или произведения, а β — отображение оценки. Тогда выполняются следующие утверждения:

а) $\mathcal{S}(t^\beta) \subseteq \mathcal{S}(t)^\beta$;

б) $|\ulcorner\beta(t)\urcorner| \leq |t|$ и $|\ulcorner\beta(t_1)\urcorner|, \ldots, |\ulcorner\beta(t_n)\urcorner| \leq |t_1, \ldots, t_n|$;

в) $|t^\beta|_{\text{ext}} \leq 2 \cdot |t|$.

Доказательство. Докажем пункты по отдельности:

(1) Доказательство ведём по структурной индукции по t.

— Если $t \in \mathcal{A}$, то $\mathcal{S}(t^\beta) = \{t\} = \mathcal{S}(t)^\beta$. Пусть $t = \langle t_1, t_2\rangle$. По индукционному предположению $S(t^\beta) = \{t^\beta\} \cup S(t_1^\beta) \cup S(t_2^\beta) \subseteq \{t^\beta\} \cup S(t_1)^\beta \cup S(t_2)^\beta = S(t)^\beta$, и тот же довод проводится для случая шифрования.

— Пусть $t = t_1^{e_1} \cdots t_n^{e_n}$. Рассмотрим два подслучая. Если $t^\beta = 1$, то очевидно $S(t^\beta) \subseteq S(t)^\beta$. Иначе по доказательству леммы 5.10 имеем $t^\beta = \prod_{j \notin J \cup \{1\}} (s_{C_j}^\beta)^{e_{C_j}}$, причём для каждого C_j найдётся t_i, такое что $t_i^\beta = s_{C_j}^\beta$. Индукция даёт

$$S(t^\beta) \subseteq \{t^\beta\} \cup \bigcup_{j \notin J \cup \{1\}} S\big(s_{C_j}^\beta\big) \subseteq \{t^\beta\} \cup \bigcup_{i=1}^{n} S(t_i)^\beta = S(t)^\beta.$$

— Если $t = \mathrm{Exp}(u, M)$ и $t^\beta = u^\beta$, то индукционное предположение немедленно даёт $S(t^\beta) \subseteq S(t)^\beta$.

— Если $t = \mathrm{Exp}(u, M)$, $t^\beta = \mathrm{Exp}(u^\beta, M^\beta)$ и $M = t_1^{e_1} \cdots t_n^{e_n}$, то $M^\beta \neq 1$ и, по индукции,

$$S(t^\beta) \subseteq \{t^\beta\} \cup S(u^\beta) \cup \bigcup_i S(t_i^\beta) \subseteq \{t^\beta\} \cup S(u)^\beta \cup \bigcup_i S(t_i)^\beta = S(t)^\beta.$$

— Если $t = \mathrm{Exp}(u, M)$, $u^\beta = \mathrm{Exp}(u', M')$ и $t^\beta = u^\beta$, то

$$S(t^\beta) \subseteq S(u^\beta) \subseteq S(u)^\beta \subseteq S(t)^\beta.$$

— Наконец, предположим, что $t = \mathrm{Exp}(u, M)$, $u^\beta = \mathrm{Exp}(u'', M'')$, а $t^\beta = \mathrm{Exp}\big(u'', (M'' \cdot M)^\beta\big)$, причём $(M'' \cdot M)^\beta \neq 1$. Тогда $(M'' \cdot M)^\beta$ имеет вид $\prod_{j \notin J \cup \{1\}} \big(s_{C_j}^\beta\big)^{e'_j}$ для некоторых показателей e'_j; при этом $M'' = t_1''^{e_1} \cdots t_n''^{e_n}$, $M = {t_1}^{e_1} \cdots {t_n}^{e_n}$, и каждый $s_{C_j}^\beta$ совпадает с некоторым t_i'' или t_i^β (заметим, что

$t''_i = t_i^\beta$ по лемме 5.11). По индукционному предположению $t''_i \in S(u^\beta) \subseteq S(u)^\beta$, откуда

$$\begin{aligned} S(t^\beta) &= \{t^\beta\} \cup S(u'') \cup \bigcup_{j \notin J \cup \{1\}} S\big(s^\beta_{C_j}\big) \\ &\subseteq \{t^\beta\} \cup S(u'') \cup \bigcup_{i=1}^{n} S\big(t_i^\beta\big) \cup \bigcup_{i=1}^{n''} S\big(t''_i\big) \\ &\subseteq \{t^\beta\} \cup \bigcup_{i=1}^{n} S\big(t_i\big)^\beta \cup S(u^\beta) \\ &\subseteq \{t^\beta\} \cup \bigcup_{i=1}^{n} S\big(t_i\big)^\beta \cup S(u)^\beta \;=\; S(t)^\beta. \end{aligned}$$

(2) Сначала заметим, что $\ulcorner \beta(t) \urcorner = \beta(t^\beta)$. Легко видеть, что для любого открытого сообщения или произведения s выполняется $|\beta(s)| \leq |s|$. Следовательно,

$$|\ulcorner \beta(t) \urcorner| = |\beta(t^\beta)| \leq |t^\beta| \overset{(*)}{\leq} \mathrm{Card}\big(S(t)^\beta\big) \leq \mathrm{Card}\big(S(t)\big) = |t|,$$

где в $(*)$ используется пункт 1. Тот же довод даёт $|\ulcorner \beta(t_1) \urcorner|, \ldots, |\ulcorner \beta(t_n) \urcorner| \leq |t_1, \ldots, t_n|$.

(3) Это непосредственное следствие пункта 1 и леммы 5.2:

$$|t^\beta|_{\mathrm{ext}} \leq 2 \cdot |t^\beta| \leq 2 \cdot \mathrm{Card}\big(S(t^\beta)\big) \leq 2 \cdot |t|. \quad \square$$

$\square$

Теперь нам нужно получить верхнюю оценку для $\|t^\beta\|_{\mathrm{exp}}$. Для этого понадобится следующая лемма.

Лемма 5.13. Пусть E — конечное множество открытых сообщений или произведений, такое что $S_{\mathrm{ext}}(E) = E$, а t — максимальный (относительно упорядочения «строгий подтерм») элемент множества E. Тогда

$$\Big|\bigcup_{s \in E} S_{\mathrm{ext}}\big(s^\beta\big)\Big|_{\mathrm{exp}} \;\leq\; \Big|\bigcup_{s \in E \setminus \{t\}} S_{\mathrm{ext}}\big(s^\beta\big)\Big|_{\mathrm{exp}} + \|t\|^2_{\mathrm{ext}}.$$

Доказательство. См. Приложение B. $\square$

Используя предыдущую лемму, получаем:

Лемма 5.14. Для всякого открытого сообщения или произведения t выполняется $\left\|t^{\beta}\right\|_{\exp} \leq \|t\|_{\text{ext}}^{3}$.

Доказательство. Положим $E = S_{\text{ext}}(t)$. По Лемме 5.13 имеем

$$\left\|t^{\beta}\right\|_{\exp} = |S_{\text{ext}}(t^{\beta})|_{\exp} \leq \Big|\bigcup_{s\in E} S_{\text{ext}}\big(s^{\beta}\big)\Big|_{\exp}.$$

Последовательно удаляя из E (максимальный) элемент и применяя Лемму 5.13 на каждом шаге, получаем $\Big|\bigcup_{s\in E} S_{\text{ext}}\big(s^{\beta}\big)\Big|_{\exp} \leq |t|_{\text{ext}} \cdot \|t\|_{\text{ext}}^{2}$, а так как $\text{Card}(E) = |t|_{\text{ext}}$, получаем требуемое неравенство $\|t^{\beta}\|_{\exp} \leq \|t\|_{\text{ext}}^{3}$. $\square$

Мы уже ограничили как количество расширенных подтермов терма t^{β}, так и величину его целых коэффициентов (см. Леммы 5.12 и 5.14). Объединив эти оценки, мы, наконец, получаем полиномиальную верхнюю границу на размер β-термов.

Лемма 5.15. Для любого открытого сообщения или произведения t выполняется

$$\left\|t^{\beta}\right\|_{\text{ext}} \leq 3 \cdot \|t\|_{\text{ext}}^{3}.$$

5.6 Ограничение размера β-систем уравнений

В предыдущем подразделе мы получили полиномиальную оценку для размера β-термов. Теперь ограничим размер β-систем уравнений, связанных с этими термами, а тем самым и общий размер β-кортежей. Для этого сначала зададим конкретную β-систему уравнений $\mathcal{E}_{t}^{\beta}$ для терма t, размер которой полиномиально ограничен величиной $\|t\|_{\text{ext}}$.

Пусть далее β — отображение оценки, а t — открытое сообщение или произведение. Опишем систему уравнений $\mathcal{E}_{t}^{'\beta}$, которая добавляется при переходе от системы, построенной для подтермов t, к системе уравнений самого t:

— Если t — атом, пара или шифрование, то $\mathcal{E}_{t}^{'\beta} = \varnothing$.

— Если $t = t_1^{e_1} \cdots t_n^{e_n}$, то, используя обозначения из доказательства Леммы 5.10, положим

$$\mathcal{E}_{t}^{'\beta} = \bigcup_{j\geq 2} \mathcal{E}_{C_j}^{\beta} \cup \bigcup_{j\in J} \{\, e_{C_j} = 0\}.$$

— Если $t = \text{Exp}(u, M)$ и $\ulcorner \beta(u) \urcorner \neq \text{Exp}(\,\cdot\,,\cdot\,)$, то $\mathcal{E}_{t}^{'\beta} = \varnothing$. В противном случае $u^{\beta} = \text{Exp}(u'', M')$ и полагаем $\mathcal{E}_{t}^{'\beta} = \mathcal{E}_{(M'':M)}^{'\beta}$.

Замечание 5.16. Система уравнений $\mathcal{E}'^{\beta}_t$ однозначно определяется (по модулю AC_+).

Система $\mathcal{E}'^{\beta}_t$ фиксирует ограничения на показатели степеней *на одном уровне* терма t. Полная β-система уравнений для t задаётся как объединение систем, построенных для всех его подтермов:

$$\mathcal{E}^{\beta}_t \;=\; \bigcup_{s\in S_{\mathrm{ext}}(t)} \mathcal{E}'^{\beta}_s.$$

Далее мы докажем, что пара $(t^\beta, \mathcal{E}^\beta_t)$ является β-кортежем для t, а также то, что размер $\mathcal{E}^\beta_t$ полиномиально ограничен размером t. Однако прежде потребуется следующая лемма о β-кортежах для произведений:

Лемма 5.17. Пусть $M = t_1^{e_1}\cdots t_n^{e_n}$ и $M' = t_1'^{e'_1}\cdots t_{n'}'^{e'_{n'}}$ — два открытых произведения такие, что $\beta(t_i) = \ulcorner\beta(t'_i)\urcorner$ для всех соответствующих множителей. Пусть для каждого i задан β-кортеж $(t_i^\beta, \mathcal{E}_i)$ терма t_i. Тогда пара

$$\Big((M'\cdot M)^\beta,\ \mathcal{E}'^{\beta}_{(M'\cdot M)} \cup \bigcup_i \mathcal{E}_i\Big)$$

является β-кортежем для произведения $M'\cdot M$.

Доказательство. Смотреть приложение В. □

Лемма 5.18. Для любого открытого сообщения или произведения t и всякого отображения оценки β выполняются следующие утверждения:

(1) Пара $\big(t^\beta, \mathcal{E}^\beta_t\big)$ является β-кортежем для t.
(2) Размер $\mathcal{E}^\beta_t$ ограничен полиномом от $\|t\|_{\mathrm{ext}}$.
(3) Общий размер $\big(t^\beta, \mathcal{E}^\beta_t\big)$, равный сумме размеров t^β и $\mathcal{E}^\beta_t$, также ограничен полиномом от $\|t\|_{\mathrm{ext}}$.

Доказательство. Докажем пункты по отдельности.

(1) Проводим структурную индукцию по t в соответствии с построением из леммы 5.10.

— Если $t \in \mathcal{A}$, случай тривиален. Предположим, что $t = \langle t_1, t_2\rangle$. Тогда $\mathcal{E}^\beta_t = \mathcal{E}'^{\beta}_t \cup \bigcup_{s\in S_{\mathrm{ext}}(t_1)} \mathcal{E}'^{\beta}_s \cup \bigcup_{s\in S_{\mathrm{ext}}(t_2)} \mathcal{E}'^{\beta}_s$. По определению имеем $\mathcal{E}^\beta_t = \mathcal{E}^\beta_{t_1} \cup \mathcal{E}^\beta_{t_2}$ (здесь используется Замечание 5.16). Точно так же, как в доказательстве леммы 5.10, отсюда следует, что $\big(t^\beta, \mathcal{E}^\beta_t\big)$ является β-кортежем для t. Рассуждение для случая шифрования проводится аналогично.

— Если $t = t_1^{e_1} \cdots t_n^{e_n}$, то, пользуясь обозначениями, введёнными в доказательстве леммы 5.10, а также определением ${\mathcal{E}'_t}^{\beta}$ и Замечанием 5.16, получаем $\mathcal{E}_t^\beta = \bigcup_{i=1}^n \mathcal{E}_{t_i}^\beta \cup \bigcup_{j=2}^\ell \mathcal{E}_{C_j}^\beta \cup \bigcup_{j\in J}\{\, e_{C_j} = 0\}$. Точно так же, как в доказательстве леммы 5.10, из этого следует, что пара $\bigl(t^\beta, \mathcal{E}_t^\beta\bigr)$ является β-кортежем для t.

— Если $t = \mathrm{Exp}(u, M)$ и $\beta(u) \neq \mathrm{Exp}(\,\cdot,\cdot\,)$, то по определению $\mathcal{E}_t^\beta$ и в силу Замечания 5.16 имеем $\mathcal{E}_t^\beta = \mathcal{E}_u^\beta \cup \mathcal{E}_M^\beta$; как и в лемме 5.10, отсюда следует, что $(t^\beta, \mathcal{E}_t^\beta)$ является β-кортежем для t.

— Наконец, пусть $t = \mathrm{Exp}(u, M)$, причём $\ulcorner\beta(u)\urcorner \neq \mathrm{Exp}(\,\cdot,\cdot\,)$ и $u^\beta = \mathrm{Exp}(u'', M'')$. Предположим, что $M = t_1^{e_1} \cdots t_n^{e_n}$. По лемме 5.17 пара $\Bigl((M''\cdot M)^\beta,\ {\mathcal{E}'}^{\beta}_{(M''\cdot M)} \cup \bigcup_i \mathcal{E}_{t_i}^\beta\Bigr)$ является β-кортежем для произведения $M''\cdot M$. По определению $\mathcal{E}_t^\beta$ и в силу Замечания 5.16 имеем $\mathcal{E}_u^\beta \cup \bigcup_i \mathcal{E}_{t_i}^\beta \cup {\mathcal{E}'}^{\beta}_{(M''\cdot M)} \subseteq \mathcal{E}_t^\beta$. Следовательно, точно так же, как в доказательстве леммы 5.10, получаем, что $\bigl(t^\beta, \mathcal{E}_t^\beta\bigr)$ является β-кортежем для t.

(2) Если t — атом, пара либо шифрование, то дополнительных оценок не требуется. Если же t является *произведением*, то из лемм 5.5 и 5.15 немедленно следует, что размер ${\mathcal{E}'_t}^{\beta}$ ограничен полиномом от $\|t\|_{\mathrm{ext}}$. Для случая $t = \mathrm{Exp}(\,\cdot,\cdot\,)$ ту же полиномиальную оценку получают, применяя лемму 5.15 совместно с уже рассмотренным случаем произведения.

(3) Пусть p — полином, ограничивающий размер ${\mathcal{E}'_t}^{\beta}$. Тогда величина $p\bigl(\|t\|_{\mathrm{ext}}\bigr)\cdot \|t\|_{\mathrm{ext}}$ ограничивает размер $\mathcal{E}_t^\beta$. Кроме того, по лемме 5.15 размер t^β также полиномиально ограничен величиной $\|t\|_{\mathrm{ext}}$. □

Наконец, леммы 5.5, 5.9 и 5.18 обеспечивают существование конкретных $\approx_\beta$-систем уравнений, чьи размеры полиномиально ограничены.

Предложение 5.19. Пусть t и t' — открытые сообщения или произведения, а β — отображение оценки, такое что $t \approx_\beta t'$. Тогда существует $\approx_\beta$-система уравнений для t и t', чей размер полиномиально ограничен величиной $\|t, t'\|_{\mathrm{ext}}$.

Такую систему уравнений будем обозначать $\mathcal{E}_{t,t'}^{\approx_\beta}$.

5.7 Ограничение величины показателей степеней в атаках

Теперь мы готовы доказать ключевую лемму этого раздела — Лемму 5.21. Как отмечалось выше, из этой леммы следует, что правила Диффи–Хеллмана позволяют осуществлять атаки, в которых показатели степеней произведений ограничены полиномом (Предложение 5.22). Немедленным следствием является то, что задача Insecure NP-полна для нарушителя DH (Теорема 5.23).

Доказательство Леммы 5.21 проводится в два этапа. Сначала рассматривается ограниченный вариант, когда применяется лишь одно правило нарушителя (Лемма 5.20); затем этот результат распространяется на полное построение вывода.

В дальнейших доказательствах нам понадобятся расширения отображений оценки. Будем говорить, что отображение $\beta' : Z' \to Z$ является *расширением* отображения оценки $\beta : Z \to Z$, если $Z \subseteq Z'$ и $\beta'(z) = \beta(z)$ для всех $z \in Z$. Так как на множестве Z отображения β и β' совпадают, то, не перегружая обозначения, расширение β будем часто обозначать тем же символом β.

Лемма 5.20. Пусть $t_1, \ldots, t_n$ — открытые сообщения, s — нормализованное сообщение, β — отображение оценки, а $L \in \mathcal{L}$ — правило нарушителя такое, что $\beta(t_i) = \ulcorner\beta(t_i)\urcorner$ для всех i и $\ulcorner\beta(t_1)\urcorner, \ldots, \ulcorner\beta(t_n)\urcorner \to s \in L$. Тогда существует открытое сообщение t, система линейных уравнений $\mathcal{E}$ и расширение β отображения β такие, что

(1) $\beta(t) = s$;
(2) $\beta \models \mathcal{E}$;
(3) $\ulcorner\beta'(t_1)\urcorner, \ldots, \ulcorner\beta'(t_n)\urcorner \to \ulcorner\beta'(t)\urcorner$ для всякого $\beta' \models \mathcal{E}$;
(4) $\max\{|e| \mid e \in \mathcal{L}_{\exp}(t)\} \leq \max\{|e| \mid e \in \mathcal{L}_{\exp}(t_1, \ldots, t_n)\} + n$;
(5) размер $\mathcal{E}$ полиномиально ограничен величиной $\|t_1, \ldots, t_n\|_{\text{ext}}$.

Доказательство. См. Приложение В. □

Лемма 5.21. Пусть $t, t_1, \ldots, t_n$ — открытые сообщения такие, что существует вывод, показывающий $\ulcorner\beta(t)\urcorner \in \text{forge}\big(\ulcorner\beta(t_1)\urcorner, \ldots, \ulcorner\beta(t_n)\urcorner\big)$. Тогда существует расширение отображения оценки β и система линейных уравнений $\mathcal{E}$ такие, что

(1) $\beta \models \mathcal{E}$;
(2) для всякого $\beta' \models \mathcal{E}$ выполняется $\ulcorner\beta'(t)\urcorner \in \text{forge}\big(\ulcorner\beta'(t_1)\urcorner, \ldots, \ulcorner\beta'(t_n)\urcorner\big)$;
(3) размер $\mathcal{E}$ полиномиально ограничен величиной $\|t_1, \ldots, t_n, t\|_{\text{ext}}$.

Доказательство. Пусть $E = \{\ulcorner\beta(t_1)\urcorner, \ldots, \ulcorner\beta(t_n)\urcorner\}$, а D — корректный вывод, свидетельствующий тому, что $\ulcorner\beta'(t)\urcorner \in \text{forge}(E)$. Известно, что длина l вывода D полиномиально ограничена величиной $|\ulcorner\beta(t_1)\urcorner, \ldots, \ulcorner\beta(t_n)\urcorner, \ulcorner\beta(t)\urcorner|$. По пункту 2 леммы 5.12 $|\ulcorner\beta(t_1)\urcorner, \ldots, \ulcorner\beta(t_n)\urcorner, \ulcorner\beta(t)\urcorner|$ ограничено полиномом от

$|t_1, \ldots, t_n, t|$, а значит и от $\|t_1, \ldots, t_n, t\|_{\text{ext}}$. Пусть i-й шаг вывода D имеет вид $E, s_1, \ldots, s_{i-1} \to_{L_i} E, s_1, \ldots, s_i, \qquad 1 \leq i \leq l$, где каждое сообщение s_i нормализовано и $s_l = \ulcorner \beta(t) \urcorner$. Поскольку вывод D корректен, для всех i выполняется $s_i \in S\big(\ulcorner \beta(t_1) \urcorner, \ldots, \ulcorner \beta(t_n) \urcorner, \ulcorner \beta(t) \urcorner\big)$.

Пусть $(t^\beta, \mathcal{E}_t^\beta)$ — β-кортеж терма t, а для каждого i задан β-кортеж t_i^β терма t_i. Тогда $\beta(t_i^\beta) = \ulcorner \beta(t_i) \urcorner$, и, следовательно, $E = \{\beta(t_1^\beta), \ldots, \beta(t_n^\beta)\}$. К первому шагу вывода D можно применить лемму 5.20, получив открытое сообщение s_1', систему уравнений $\mathcal{E}_1$ и расширение отображения оценки β такие, что $\beta(s_1') = s_1$, $\beta \models \mathcal{E}_1$ и $\ulcorner \beta'(t_1^\beta) \urcorner, \ldots, \ulcorner \beta'(t_n^\beta) \urcorner \xrightarrow{L_1} \ulcorner \beta'(t_1^\beta) \urcorner, \ldots, \ulcorner \beta'(t_n^\beta) \urcorner, \ulcorner \beta'(s_1') \urcorner$ для всякого $\beta' \models \mathcal{E}_1$.

Заметим, что для каждого i выполняется $\beta(t_i^\beta) = \ulcorner \beta(t_i^\beta) \urcorner$, а также $\beta(s_1') = \ulcorner \beta(s_1') \urcorner = s_1$. Следовательно, лемму 5.20 можно применять индуктивно. Для каждого шага j $(1 \leq j \leq l)$ получаем открытое сообщение s_j', систему уравнений $\mathcal{E}_j$ и расширение отображения оценки β такие, что

$\beta(s_j') = s_j, \beta \models \mathcal{E}_j, \ulcorner \beta'(t_1^\beta) \urcorner, \ldots, \ulcorner \beta'(t_n^\beta) \urcorner, \ulcorner \beta'(s_1') \urcorner, \ldots, \ulcorner \beta'(s_{j-1}') \urcorner \to_{L_j} \ulcorner \beta'(t_1^\beta) \urcorner, \ldots, \ulcorner \beta'(t_n^\beta) \urcorner, \ulcorner \beta'(s_1') \urcorner, \ldots, \ulcorner \beta'(s_j') \urcorner$ для всякого $\beta' \models \mathcal{E}_j$. Следовательно, $\beta \models \bigcup_{j=1}^{l} \mathcal{E}_j$ и $\ulcorner \beta'(s_l') \urcorner \in \text{forge}\big(\ulcorner \beta'(t_1^\beta) \urcorner, \ldots, \ulcorner \beta'(t_n^\beta) \urcorner\big)$ для всякого $\beta' \models \bigcup_{j=1}^{l} \mathcal{E}_j$.

Если $\beta' \models \bigcup_{i=1}^{n} \mathcal{E}_{t_i}^\beta$, то $\ulcorner \beta'(t_i) \urcorner = \ulcorner \beta'(t_i^\beta) \urcorner$ для всех i. Поскольку $\beta(t^\beta) = \ulcorner \beta(t) \urcorner = s_l = \beta(s_l')$, получаем $t^\beta =_\beta s_l'$. Следовательно, по лемме 5.5 существует $=_\beta$-система уравнений $\mathcal{E}_{t^\beta, s_l'}^{=_\beta}$ для t^β и s_l'.

Теперь, если $\beta' \models \mathcal{E}_t^\beta \cup \mathcal{E}_{t^\beta, s_l'}^{=_\beta}$, имеем $\ulcorner \beta'(t) \urcorner = \ulcorner \beta'(t^\beta) \urcorner = \ulcorner \beta'(s_l') \urcorner$.. Положим

$$\mathcal{E} = \bigcup_{i=1}^{n} \mathcal{E}_{t_i}^\beta \cup \mathcal{E}_t^\beta \cup \bigcup_{j=1}^{l} \mathcal{E}_j \cup \mathcal{E}_{t^\beta, s_l'}^{=_\beta}.$$

Отсюда имеем $\beta \models \mathcal{E}$ и $\ulcorner \beta'(t) \urcorner \in \text{forge}\big(\ulcorner \beta'(t_1) \urcorner, \ldots, \ulcorner \beta'(t_n) \urcorner\big)$ для любого $\beta' \models \mathcal{E}$.

Остаётся показать, что размер $\mathcal{E}$ полиномиально ограничен величиной $\|t_1, \ldots, t_n, t\|_{\text{ext}}$. По лемме 5.20 каждый $\mathcal{E}_j$ полиномиально ограничен в $\|t_1, \ldots, t_n, s_1', \ldots, s_{j-1}'\|_{\text{ext}}$. Заметим, что $\beta(s_j') = s_j \in S\big(\ulcorner \beta(t_1) \urcorner, \ldots, \ulcorner \beta(t_n) \urcorner, \ulcorner \beta(t) \urcorner\big)$. Следовательно, по лемме 5.12 $|s_j'|$ полиномиально ограничено в $|t_1, \ldots, t_n, t|$, а по лемме 5.2 то же верно и для $|s_j'|_{\text{ext}}$.

Из леммы 5.20 получаем

$$\max\{|e| \mid e \in \mathcal{L}_{\exp}(s'_j)\} \;\leq\; \max\{|e| \mid e \in \mathcal{L}_{\exp}(t_1^\beta, \ldots, t_n^\beta)\} + n\,(j-1).$$

Поскольку $j \leq l$, а длина l вывода полиномиально ограничена значением $\|t_1, \ldots, t_n, t\|_{\text{ext}}$, и, кроме того, $\max\{|e| \mid e \in \mathcal{L}_{\exp}(t_1^\beta, \ldots, t_n^\beta)\} \leq \|t_i\|_{\text{ext}}^3$ для некоторого i (лемма 5.14), существует полином p такой, что $\|s'_j\|_{\text{ext}} \leq p\big(\|t_1, \ldots, t_n, t\|_{\text{ext}}\big)$. Отсюда

$$\|t_1, \ldots, t_n, t, s'_1, \ldots, s'_j\|_{\text{ext}} \;\leq\; \big(p'(\|t_1, \ldots, t_n, t\|_{\text{ext}}) + 1\big)\, p\big(\|t_1, \ldots, t_n, t\|_{\text{ext}}\big),$$

где p' — полином, ограничивающий l. По лемме 5.20 это означает, что каждый $\mathcal{E}_j$ полиномиально ограничен в $\|t_1, \ldots, t_n, t\|_{\text{ext}}$. Леммы 5.18 и 5.5 теперь дают, что и $\mathcal{E}$ в целом полиномиально ограничена той же величиной.

□

Теперь мы можем показать, что правила Диффи–Хеллмана допускают атаки, в которых показатели степеней произведений остаются полиномиально ограниченными.

Предложение 5.22 Правила DH допускают атаки с полиномиально ограниченными показателями степеней произведений.

Доказательство. Пусть (π, σ) — минимальная атака на протокол P. Обозначим через σ^Z подстановку, полученную из σ заменой *всех* показателей степеней на новые переменные. Положим, что отображение оценки β сопоставляет каждой из этих переменных соответствующий показатель произведения, то есть $\sigma(x) = \beta\big(\sigma^Z(x)\big)$ для любого $x \in \mathcal{V}(P)$. По следствию 3.16 длина $|\sigma^Z|$ полиномиально ограничена величиной $|P|$. Так как в σ^Z показатели степеней являются переменными, получаем $\|\sigma^Z\|_{\exp} \leq |\sigma^Z|^2$. Следовательно, $\|\sigma^Z\|_{\text{ext}}$ полиномиально ограничена величиной $\|P\|_{\text{ext}}$. □

Пусть $k, R_1, \ldots, R_k, S_0, \ldots, S_k$ определены, как и раньше. Без ограничения общности будем считать, что S_0 состоит из одного сообщения, а не из множества сообщений (иначе запишем $S_0 = \{a_1, \ldots, a_n\}$ в виде $\langle a_1, (a_2 \ldots (a_{n-1}, a_n) \ldots)\rangle$). Положим $R_{k+1} = \mathit{secret}$. Известно, что

$$\beta\big(\ulcorner R_i\sigma^Z \urcorner\big) \;\in\; \text{forge}\big(\ulcorner \beta(S_0\sigma^Z) \urcorner, \ldots, \ulcorner \beta(S_{i-1}\sigma^Z) \urcorner\big), \qquad 1 \leq i \leq k+1.$$

По лемме 5.21 для каждого i существует расширение отображения оценки β (причём все такие расширения независимы друг от друга) и система линейных уравнений $\mathcal{E}_i$ такие, что

– $\beta \models \mathcal{E}_i$;

– для любого $\beta' \models \mathcal{E}_i$ выполняется

$$\ulcorner \beta'(R_i \sigma^Z) \urcorner \in \mathrm{forge}\big(\ulcorner \beta'(S_0 \sigma^Z) \urcorner, \ldots, \ulcorner \beta'(S_{i-1} \sigma^Z) \urcorner\big);$$

– размер $\mathcal{E}_i$ полиномиально ограничен значением $\|S_0\sigma^Z, \ldots, S_k\sigma^Z, R_1\sigma^Z, \ldots, R_{k+1}\sigma^Z\|_{\mathrm{ext}}$, которое, в свою очередь, полиномиально ограничено величиной $\|P\|_{\mathrm{ext}}$.

Следовательно, $\beta \models \bigcup_{i=1}^{k} \mathcal{E}_i =: \mathcal{E}$; отсюда система $\mathcal{E}$ разрешима, и для всякого $\beta' \models \mathcal{E}$ пара $\big(\pi, \beta'(\sigma^Z)\big)$ представляет собой атаку на P. По результату [23] существует решение β' системы $\mathcal{E}$, для которого двоичная запись всех целых коэффициентов полиномиально ограничена размером $\mathcal{E}$; следовательно, благодаря лемме 5.21 эта запись полиномиально ограничена величиной $\|P\|_{\mathrm{ext}}$. Определим $\sigma' := \beta'(\sigma^Z)$; тогда (π, σ') является атакой на P. Так же $\sigma \approx \sigma'$, то есть подстановки σ и σ' различаются лишь показателями степеней, а величина $\|\sigma'\|_{\mathrm{exp}}$ полиномиально ограничена $\|P\|_{\mathrm{ext}}$ и, по лемме 5.2, $\|P\|$. □

Теорема 5.23. Задача Insecure NP-полна для нарушителя DH.

6 Протокол A–GDH.2

Протокол A–GDH.2, предложенный в работе [22], позволяет группе участников, обладающих попарными долгосрочными ключами, установить общий сеансовый ключ с помощью возведения в степень по Диффи–Хеллману. Подробное описание протокола можно найти в [22].

Пусть $P = \{1, \ldots, n, I\}$ — множество субъектов, которые могут участвовать в одном запуске протокола A–GDH.2, где I обозначает нарушителя (нарушитель может быть как честным, так и нечестным субъектом). Любая пара участников $i, j \in P$ разделяет долгосрочный общий ключ $K_{ij} (= K_{ji})$. В одном протокольном запуске некоторая подгруппа $G \subseteq P$ субъектов (состав группы может меняться от запуска к запуску) должна выработать сеансовый ключ, известный только членам группы G, при условии, что все субъекты из G честны (неявная аутентификация сеансового ключа). В ходе выполнения протокола один из субъектов играет роль так называемого *мастера*. Предположим, к примеру, что $A, B, C, D \in P$ хотят разделить сеансовый ключ и что мастером является D. Тогда A посылает сообщение B, B — сообщение C, а C — сообщение мастеру D. После этого D вычисляет сеансовый ключ для себя и распространяет вспомогательный материал, позволяющий A, B, C, используя свои долгосрочные ключи с другими субъектами, получить тот же сеансовый ключ. Обозначим A первым, B — вторым, а C — третьим участником группы.

Теперь дадим формальное описание протокола в нашей модельной схеме. Термы $(t_1\langle t_2 \ldots \langle t_{n-1}, t_n\rangle \ldots\rangle)$ будем сокращённо записывать как $t_1, \ldots, t_n$. Для $l \in \{1, 2\}$ положим, что $\Pi_{p,p'}^{l,j}$ — это l-й шаг субъекта $p \in P$ в j-м экземпляре протокола, $j \geq 0$, когда p действует как l-й участник группы, а $p' \in P$ является мастером. Отношение $\Pi_{p,p'}^{1,j} < \Pi_{p,p'}^{2,j}$ — единственное непустое отношение частичного порядка между правилами.

Через $r^{\,p,j}$ обозначим случайное число (атомарное сообщение), сгенерированное субъектом p в j-м экземпляре, а $secret^{\,p,j}$ — секрет (некоторое атомарное сообщение) того же субъекта p.

Определим $\Pi_{p,p'}^{1,j}$ — первый шаг субъекта p в экземпляре j, когда p выступает первым участником группы (то есть инициатором протокола), а p' — мастером:

$$1 \;\Rightarrow\; \alpha,\; Exp\big(\alpha, r^{\,p,j}\big),$$

где α — порождающий элемент группы (атомарное сообщение). Для $i > 1$ первое правило $\Pi^{p,j}_{i,1,p'}$ определяется так:

$$x_1^{p,j}, \ldots, x_i^{p,j} \implies \mathrm{Exp}\big(x_1^{p,j}, r^{\,p,j}\big),\ \ldots\ , \mathrm{Exp}\big(x_{i-1}^{p,j}, r^{\,p,j}\big),\ x_i^{p,j},\ \mathrm{Exp}\big(x_i^{p,j}, r^{\,p,j}\big),$$

где все $x_k^{p,j}$ являются переменными. Второй шаг $\Pi^{p,j}_{i,2,p'}$ участника p в экземпляре j (при $i > 0$) задаётся правилом

$$y^{p,j} \implies \big\{ secret^{\,p,j} \big\}^{s}_{\mathrm{Exp}\left(y^{\,p,j},\, r^{\,p,j} K^{-1}_{p',p}\right)},$$

Заметим, что $\mathrm{Exp}(y^{\,p,j},\ r^{\,p,j} K^{-1}_{p,p})$ есть сеансовый ключ, вычисляемый субъектом p; условие неявной аутентификации ключа требует, чтобы ни один участник, не входящий в группу, не смог получить $secret^{\,p,j}$.

Определим протокольное правило $M^{p,j}_{p_1 \ldots p_h}$, описывающее поведение субъекта $p \in P$ в j-м экземпляре как мастера группы $p_1, \ldots, p_h, p$ (в указанном порядке), где p — последний член группы. Положим

$$M^{p,j}_{p_1 \ldots p_h} := z_1^{p,j}, \ldots, z_{h+1}^{p,j} \implies \mathrm{Exp}\big(z_1^{p,j},\, r^{\,p,j} \cdot K_{p_1,p}\big), \ldots, \mathrm{Exp}\big(z_h^{p,j},\, r^{\,p,j} \cdot K_{p_h,p}\big), \big\{ secret^{\,p,j} \big\}^{s}_{\mathrm{Exp}(z_{h+1}^{p,j},\, r^{\,p,j})},$$

где $z_k^{p,j}$ — переменные, $\mathrm{Exp}(z_k^{p,j},\, r^{\,p,j} \cdot K_{p_k,p})$ служат ключевым материалом для p_k, а сообщение $\mathrm{Exp}(z_{h+1}^{p,j}, r^{\,p,j})$ является сеансовым ключом, вычисленным мастером p.

Ниже задаётся протокол P, который описывает два запуска схемы A–GDH.2: первый — для группы $p, p', I, p'' \in P$, и второй — для группы p, p', p'', причём в обоих случаях мастером является p''. В первом запуске действия нарушителя I можно не специфицировать. Формально множество правил протокола P состоит из следующих выражений: правила участника p в первом сеансе $\Pi^{p,1}_{1,1,p''}$ и $\Pi^{p,1}_{1,2,p''}$ (причём $\Pi^{p,1}_{1,1,p''} < \Pi^{p,1}_{1,2,p''}$), правила участника p' в том же сеансе $\Pi^{p',1}_{2,1,p''}$ и $\Pi^{p',1}_{2,2,p''}$, а также правило мастера $M^{p'',1}_{pp'I}$; правила второго сеанса — $\Pi^{p,2}_{1,1,p''}$, $\Pi^{p,2}_{1,2,p''}$, $\Pi^{p',2}_{2,1,p''}$, $\Pi^{p',2}_{2,2,p''}$ и $M^{p'',2}_{pp'}$. Начальные знания нарушителя равны $\{\alpha, r^{I,1}\} \cup \{K_{pI} \mid p \in P\}$. Пусть $secret$ — один из секретов, выдаваемых p или p' во втором сеансе. Поскольку нарушитель не входит во вторую группу, он не должен получить $secret$. Однако, как показано в [10], для P существует атака, и нетрудно убедиться, что наша процедура вывода её обнаружит.

7 Перенос результатов на коммутативное шифрование с открытым ключом

В этом разделе мы переносим результаты, полученные в §4 и §5 для возведения в степень Диффи–Хеллмана, на коммутативное шифрование с открытым ключом (например, RSA с общим модулем). Покажем, что задача Insecure остаётся $\overline{\text{NP}}$-полной, а задача вывода — т.е. определение, выводится ли данное сообщение из конечного набора сообщений — может решаться эффективно. Эти результаты достигаются при небольшой модификации моделей и доказательств, представленных выше. Возможность переноса объясняется тем, что возведение в степень Диффи–Хеллмана и коммутативное шифрование с открытым ключом (в случае RSA также основанное на возведении в степень) обладают сходными алгебраическими свойствами. Будем интерпретировать операцию возведения в степень $c = \text{Exp}(m, k_A)$ как шифрование сообщения m публичным ключом k_A, где k'_A — соответствующий закрытый ключ. Вычисляя $\text{Exp}(c, k'_A) = \text{Exp}(m, k_A \cdot k'_A) = \text{Exp}(m, 1) = m$, мы расшифровываем c и получаем открытый текст m. Коммутативность шифрования даёт эквивалентность $\text{Exp}(\text{Exp}(m, k_A), k_B)$ и $\text{Exp}(\text{Exp}(m, k_B), k_A)$ в рамках рассматриваемых алгебраических свойств. Из-за такого толкования возведения в степень при коммутативном шифровании возникают некоторые отличия.

Во-первых, возможности нарушителя различаются. При коммутативном шифровании с открытым ключом нарушитель не в состоянии вычислять обратные показатели степени: имея публичный ключ (n, e) и шифртекст $c \equiv m^e \pmod{n}$, он не может найти закрытый ключ d и затем, вычислив $c^d \bmod n$, восстановить сообщение m. Напротив, в случае Диффи–Хеллмана возведение в степень выполняется по модулю общедоступного простого числа, поэтому нарушитель может эффективно получить обратный показатель. Например, имея $m = g^{a \cdot b}$ и b (где g порождает мультипликативную группу по модулю p), он вычисляет обратный элемент b^{-1} по модулю $p - 1$ (если обратный существует) и получает $m^{b^{-1}} = g^a$.

Во-вторых, в рассмотренной ранее модели нарушитель не располагает явными обратными элементами сообщений, такими как b^{-1}, поскольку его знания ограничены стандартными сообщениями. Однако в модели коммутативного шифрования с открытым ключом такое ограничение слишком жёстко: обратные элементы соответствуют закрытым ключам, и мы должны разрешить нарушителю владеть этими ключами — как собственными, так и ключами нечестных участников.

Ниже мы приведём два простых примера, демонстрирующих применение коммутативных схем шифрования с открытым ключом в криптографических протоколах, затем обозначим изменения, необходимые в наших моделях протокола и нарушителя, и, наконец, сформулируем основные результаты данного раздела.

7.1 Примеры протоколов, использующих коммутативное шифрование с открытым ключом

Два следующих примера заимствованы из книги [24]. Первый протокол принадлежит Шамиру. Его цель — обеспечить защищённую связь между двумя агентами, которые не делят симметрический ключ и не знают открытый ключ друг друга. Протокол опирается на коммутативность шифрования в системе RSA и состоит из трёх сообщений:

$$
\begin{aligned}
&1.\ \ A \rightarrow B:\ \ Exp(secret, K_A)\\
&2.\ \ B \rightarrow A:\ \ Exp\big(Exp(secret, K_A), K_B\big)\\
&3.\ \ A \rightarrow B:\ \ Exp(secret, K_B)
\end{aligned}
$$

В протоколе предполагается общий модуль n (типичен для RSA). Публичный ключ A — пара (n, K_A), публичный ключ B — пара (n, K_B). Сообщение *secret* есть неотрицательное целое, меньшее n; выражение $Exp(secret, K_A)$ обозначает $secret^{\,K_A} \bmod n$. Благодаря алгебраическим свойствам возведения в степень имеем $Exp\big(Exp(secret, K_A), K_B\big) = Exp(secret, K_A \cdot K_B) = Exp\big(Exp(secret, K_B), K_A\big)$.

На шаге 3 участник A вычисляет $Exp\Big(Exp\big(Exp(secret, K_A), K_B\big), K'_A\Big) = Exp(secret, K_A \cdot K_B \cdot K'_A) = Exp(secret, K_B)$, где K'_A — закрытый ключ A. Протокол, тем самым, сам использует коммутативность шифрования. Поскольку B в протоколе никак не аутентифицируется, нарушитель способен выдать себя за B, просто играя роль B и используя собственный открытый ключ K_I. Таким образом, протокол уязвим, и эта атака легко обнаруживается нашей процедурой вывода.

Коммутативная система шифрования с открытым ключом (или схема подписи) может оказаться полезной и в групповых протоколах. По мотивам описанного в [24, гл. 23] протокола рассмотрим группу из l агентов. Доверенный сервер генерирует два больших простых числа p и q, вычисляет $n = p \cdot q$ и подбирает $l + 1$ чисел $k_0, \ldots, k_l$ так, что

$$k_0 \cdots k_l \equiv 1 \pmod{(p-1)(q-1)}.$$

Каждому агенту A_i, $1 \le i \le l$, для каждого j выдаются публичные ключи K_j, равные произведению всех $k_0 \ldots k_l$, кроме k_j, и собственный закрытый ключ k_i. При этом

$$Exp\big(M,\, k_0 \cdots k_l\big) = M,$$

и, в частности,

$$Exp\big(Exp(M, k_i), K_i\big) = Exp\big(M,\, k_i \cdot K_i\big) = M.$$

После того как распределение ключей завершено, сообщение может быть подписано подмножеством членов группы $\{A_i \mid i \in \{1, \ldots, l\}\}$. Предположим, к примеру, что $l = 4$ и A_1 хочет подписать документ M совместно с A_2 и A_4. Возможная последовательность сообщений такова:

1. $A_1 \to A_2 : Exp(M, k_1)$;
2. $A_2 \to A_4 : Exp\big(Exp(M, k_1), k_2\big)$;
3. $A_4 \to A_1 : Exp\big(Exp\big(Exp(M, k_1), k_2\big), k_4\big)$.

Получив второе сообщение, агент A_4 может проверить подписи и личности агентов, подписавших M, проверив равенство

$$Exp\Big(Exp\Big(Exp\big(Exp(M, k_1), k_2\big), K_1\Big), K_2) = Exp\big(M,\, k_1 \cdot K_1 \cdot k_2 \cdot K_2\big) = M.$$

После этого A_4 при желании подписывает контракт своим закрытым ключом k_4. Важно, что благодаря коммутативности операции шифрования A_4 необязательно знать порядок, в котором остальные участники накладывали подписи. Разумеется, если рассматривать указанный обмен как протокол подписания контракта, то у него возникает множество проблем; однако их обсуждение выходит за рамки данной работы.

7.2 Модель протокола и нарушителя для схем с коммутативным шифрованием

Ниже мы формально определяем нашу модель, задавая понятия термов, сообщений, протоколов, нарушителя и атак.

Термы и сообщения. Определения близки к приведённым в § 2.1. Оператор открытого-ключевого шифрования $\{m\}_{k^P}$ опускается, поскольку теперь его заменяет форма $Exp(m, k)$. При желании этот оператор можно было бы сохранить, чтобы моделировать некоммутативное шифрование, но ради краткости мы его опустим. Главное отличие состоит в том, что показатели степеней ограничены только неотрицательными целыми — это обусловлено тем, что, в отличие от ситуации Диффи–Хеллмана, инвертирование показателей здесь вычислительно неосуществимо (см. ниже дополнительное пояснение).

Формально задаём

$$\begin{aligned} \mathit{term} &::= \mathcal{A} \mid \mathcal{V} \mid \langle \mathit{term}, \mathit{term} \rangle \mid \{\mathit{term}\}^s_{\mathit{term}} \mid \mathit{Exp}(\mathit{term}, \mathit{product}), \\ \mathit{product} &::= \mathit{term}^{\mathbb{N}} \mid \mathit{term}^{\mathbb{N}} \cdot \mathit{product}, \end{aligned}$$

где $\mathcal{A}$ — конечное множество констант (атомарных сообщений), включающее имена субъектов, одноразовые числа, ключи, а также константы 1 и *secret*; $\mathcal{K} \subseteq \mathcal{A}$ — подмножество, содержащее все открытые и закрытые ключи; $\mathcal{V}$ — конечное множество переменных; $\mathbb{N}$ — множество неотрицательных целых. Предполагается наличие биекции $\cdot' : \mathcal{K} \to \mathcal{K}$, которая каждому открытому (закрытому) ключу k сопоставляет соответствующий закрытый (открытый) ключ k'.

Как отмечалось, оператор $Exp(\,\cdot\,,\cdot\,)$ теперь интерпретируется как коммутативное шифрование с открытым ключом. Поэтому показатели степеней в произведениях ограничиваются неотрицательными целыми: расшифровать сообщение $Exp(m, k)$ без знания закрытого ключа k' практически невозможно даже

при наличии открытого ключа k. Напомним, что в модели Диффи–Хеллмана, получив k, любой — включая нарушителя — мог вычислить k^{-1} и тем самым восстановить исходное сообщение: $Exp\big(Exp(m,k),k^{-1}\big) = Exp\big(m,\, k\cdot k^{-1}\big) = Exp(m,1) = m$. Однако, если субъект располагает *закрытым* ключом k', он способен «обратить» показатель степени. Чтобы отразить это, мы рассматриваем закрытые ключи как атомарные сообщения k' (а не как формальные обратные элементы k^{-1}) и расширяем функцию нормализации так, чтобы в показателях степеней открытые и соответствующие им закрытые ключи сокращались. Иными словами, $Exp\big(Exp(m,k),k'\big) = Exp\big(m,k\cdot k'\big) = Exp(m,1) = m$.

Более формально, мы фиксируем следующий набор алгебраических свойств. Они включают свойства, принятые для возведения в степень Диффи–Хеллмана (§ 2.1), и дополнительно тождество $k\cdot k' = 1$, где k' — закрытый (открытый) ключ, соответствующий открытому (закрытому) ключу k. Таким образом, наряду с коммутативностью и ассоциативностью оператора произведения мы предполагаем следующие равенства:

$$
\begin{array}{lll}
t^1 = t & t\cdot 1 = t & Exp(t,1) = t \\
t^0 = 1 & t^z\cdot t^{z'} = t^{\,z+z'} & Exp\big(Exp(t,M_1),M_2\big) = Exp(t,M_1\cdot M_2) \\
1^z = 1 & k\cdot k' = 1 &
\end{array}
$$

где t — стандартный терм, M_1, M_2 — произведения, $k, k' \in \mathcal{K}$ определены выше, а z, z' — неотрицательные целые.

Нормальной формой $\ulcorner t \urcorner$ терма t (как и в случае возведения в степень Диффи–Хеллмана) называется результат исчерпывающего применения приведённых выше тождеств «слева направо». Нормальная форма однозначно определяется с точностью до коммутативности и ассоциативности оператора произведения. Термы t и t' считаются *эквивалентными*, если $\ulcorner t \urcorner = \ulcorner t' \urcorner$. Понятие нормальной формы естественно распространяется на множества термов и подстановки.

Ниже приведены примеры нормализации; пусть $a, b, c, d \in \mathcal{K}$:

(1) $\ulcorner (a^2\cdot b)\cdot b^2 \urcorner = a^2\cdot b'$,

(2) $Exp\big(Exp(a,(b^1\cdot c)^{\,1}),c^{\,d^2}\big) = Exp(a, b\cdot d^2)$,

(3) $Exp\big(Exp\big(Exp(a,b^3\cdot c^{\,6}),b^5\big),c^5\big) = a$.

Заметим, что, например, b' обозначает закрытый ключ, соответствующий открытому ключу b.

Протоколы. Протоколы определяются так же, как в Определении 2.6.

В нашей модели протоколов RSA-процедура (пункт 7.1) формально задаётся следующим образом: предположим, что A выполняет один экземпляр протокола как инициатор, а B — один экземпляр как респондент. Протокол состоит из трёх правил, обозначаемых $(A,1)$, $(A,2)$ и $(B,1)$:

$$\begin{aligned}(A,1):&\quad 1 \implies Exp(secret, K_A),\\ (A,2):&\quad x \implies Exp(x, K'_A),\\ (B,1):&\quad y \implies Exp(y, K_B),\end{aligned}$$

где $(A,1)$ и $(A,2)$ — первый и второй шаги агента A, а $(B,1)$ — шаг агента B. Частичный порядок задаётся множеством $\leqslant = \{((A,1),(A,2))\}$, то есть единственным требованием $(A,1) < (A,2)$; это гарантирует, что правило $(A,1)$ должно быть выполнено до $(A,2)$. Начальные знания нарушителя равны $\{1,\ K_I,\ K'_I\}$; помимо константы 1 нарушитель знает свой открытый и закрытый ключи.

Модель нарушителя и атаки. Пусть E — конечное нормализованное множество сообщений. Множество сообщений $forge(E)$, которые нарушитель может вывести из E, определяется так же, как и для возведения в степень Диффи–Хеллмана, за исключением того, что показатели z_i, возникающие в оракульных правилах, теперь ограничены неотрицательными целыми (см. Определение 4.1). Нарушителя, получаемого таким образом, далее будем называть *RSA-нарушителем.*

Понятия атаки и задачи Insecure вводятся, как и прежде (см. Определение 2.8). Нетрудно проверить, что формально специфицированный выше протокол является по нашей дефиниции небезопасным.

7.3 Основные результаты для протоколов с коммутативным шифрованием

Ниже приведены результаты, которые переносятся из случая возведения в степень Диффи–Хеллмана практически без изменений.

Теорема 7.1 (7.1)**.** Для RSA-нарушителя задача Derive решается за детерминированное полиномиальное время.

Доказательство повторяет рассуждения для DH-нарушителя.

Теорема 7.2 (7.2)**.** Для RSA-нарушителя задача INSECURE является NP-полной.

Главное отличие от доказательства для DH-нарушителя состоит в том, что теперь мы сводим проблему небезопасности не к решению линейных уравнений в целых, а в *неотрицательных* целых. Поскольку, согласно [25], размер решений можно полиномиально ограничить через размер самой системы, мы попрежнему получаем полиномиальную оценку размера подстановки, необходимой для атаки, а значит — NP-алгоритм решения. NP-трудность устанавливается так же, как и раньше.

ЗАКЛЮЧЕНИЕ

Мы показали, что задача проверки небезопасности для протоколов, использующих возведение в степень Диффи–Хеллмана с произвольными произведениями в показателях, является NP-полной и что в этой модели задача вывода может быть решена за детерминированное полиномиальное время. Кроме того, продемонстрировано, каким образом эти результаты переносятся на протоколы, основанные на коммутативном шифровании с открытым ключом.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Dolev D., Yao A. On the Security of Public-Key Protocols // IEEE Transactions on Information Theory. — 1983. — Т. 29, № 2. — С. 198—208.

2. Meadows C. Open issues in formal methods for cryptographic protocol analysis // Proceedings of DISCEX 2000. — IEEE Computer Society Press, 2000. — С. 237—250.

3. Amadio R., Lugiez D., Vanackere V. On the symbolic reduction of processes with cryptographic functions // Theoretical Computer Science. — 2002. — Т. 290, № 1. — С. 695—740.

4. Millen J. K., Shmatikov V. Constraint solving for bounded-process cryptographic protocol analysis // Proceedings of the 8th ACM Conference on Computer and Communications Security. — ACM Press, 2001. — С. 166—175.

5. Clark J., Jacob J. A Survey of Authentication Protocol Literature. — 1997. — Web Draft Version 1.0, http://citeseer.nj.nec.com/.

6. Boyd C., Mathuria A. Protocols for Authentication and Key Establishment. — Springer, 2003.

7. Bull J., Otway D. The authentication protocol : тех. отч. / Defence Research Agency. — Malvern, UK, 1997. — DRA/CIS3/PROJ/CORBA/SC/1/CSM/436—04/03.

8. Paulson L. Mechanized Proofs for a Recursive Authentication Protocol // 10th IEEE Computer Security Foundations Workshop (CSFW-10). — IEEE Computer Society Press, 1997. — С. 84—95.

9. Ryan P., Schneider S. An Attack on a Recursive Authentication Protocol // Information Processing Letters. — 1998. — Т. 65, № 1. — С. 7—10.

10. Pereira O., Quisquater J.-J. A Security Analysis of the Cliques Protocols Suites // 14th IEEE Computer Security Foundations Workshop (CSFW-14). — IEEE Computer Society, 2001. — С. 73—81.

11. An NP Decision Procedure for Protocol Insecurity with XOR / Y. Chevalier [и др.] // Proceedings of the Eighteenth Annual IEEE Symposium on Logic in Computer Science (LICS 2003). — IEEE Computer Society, 2003. — С. 261—270.

12. Comon-Lundh H., Shmatikov V. Intruder deductions, constraint solving and insecurity decision in presence of exclusive or // Proceedings of the Eighteenth Annual IEEE Symposium on Logic in Computer Science (LICS 2003). — IEEE Computer Society, 2003. — С. 271—280.

13. Meadows C., Narendran P. A Unification Algorithm for the Group Diffie–Hellman Protocol // Workshop on Issues in the Theory of Security (WITS 2002). — 2002.

14. Kapur D., Narendran P., Wang L. Analyzing protocols that use modular exponentiation: Semantic unification techniques // Proceedings of the 14th International Conference on Rewriting Techniques and Applications (RTA 2003). Т. 2706 / под ред. R. Nieuwenhuis. — Springer, 2003. — С. 165—179. — (Lecture Notes in Computer Science).

15. Pereira O., Quisquater J.-J. Generic Insecurity of Cliques-Type Authenticated Group Key Agreement Protocols // 17th IEEE Computer Security Foundations Workshop (CSFW-17). — IEEE Computer Society Press, 2004. — С. 16—29.

16. Goubault-Larrecq J., Roger M., Verma K. Abstraction and resolution modulo AC: How to verify Diffie–Hellman-like protocols automatically. — 2005. — Journal of Logic and Algebraic Programming, to appear.

17. Boreale M., Buscemi N. On the Symbolic Analysis of Low-Level Cryptographic Primitives: Modular Exponentiation and the Diffie–Hellman Protocol // Workshop on Foundations of Computer Security (FCS 2003). — 2003.

18. Millen J., Shmatikov V. Symbolic Protocol Analysis with Products and Diffie–Hellman Exponentiation // 16th IEEE Computer Security Foundations Workshop (CSFW 16). — IEEE Computer Society, 2003. — С. 47—61.

19. Shmatikov V. Decidable Analysis of Cryptographic Protocols with Products and Modular Exponentiation // 13th European Symposium on Programming (ESOP 2004). Т. 2986 / под ред. D. Schmidt. — Springer, 2004. — С. 355—369. — (Lecture Notes in Computer Science).

20. Deciding the Security of Protocols with Diffie–Hellman Exponentiation and Products in Exponents / Y. Chevalier [и др.] // Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2003). Т. 2914 / под ред. P. Pandya, J. Radhakrishnan. — Springer, 2003. — С. 124—135. — (Lecture Notes in Computer Science).

21. Rusinowitch M., Turuani M. Protocol Insecurity with Finite Number of Sessions is NP-complete // 14th IEEE Computer Security Foundations Workshop (CSFW-14). — IEEE Computer Society, 2001. — С. 174—190.

22. Steiner M., Tsudik G., Waidner M. CLIQUES: A new approach to key agreement // IEEE International Conference on Distributed Computing Systems. — IEEE Computer Society Press, 1998. — С. 380—387.

23. Bockmayr A., Weispfenning V. Solving numerical constraints // Handbook of Automated Reasoning. Т. I / под ред. A. Robinson, A. Voronkov. — Elsevier Science, 2001. — Гл. 12. С. 751—842.

24. Schneier B. Applied Cryptography. — New York : John Wiley & Sons, 1996.

25. Borsh I., Treybig L. Bounds on positive integral solutions of linear diophantine equations // Proceedings of the American Mathematical Society. — 1976. — Т. 55. — С. 299—304.

ПРИЛОЖЕНИЕ А

Характеризация сомножителей минимальных атак

Лемма 3.4 Пусть u — нормализованный терм, а M и M' — два произведения такие, что для любого $t \in \mathcal{F}(M)$ ($t \in \mathcal{F}(M')$, терм t нормализован. Пусть s — стандартный нормализованный терм и δ — замена $[s \leftarrow 1]$. Тогда

а) $\ulcorner(M \cdot M')\delta\urcorner = \ulcorner\ulcorner M \cdot M'\urcorner\delta\urcorner$; в частности $\ulcorner M\delta\urcorner = \ulcorner\ulcorner M\urcorner\delta\urcorner$;

б) $\ulcorner Exp(u, M)\delta\urcorner = \ulcorner\ulcorner Exp(u, M)\urcorner\delta\urcorner$ если $s \neq \ulcorner Exp(u, M)\urcorner$, и, кроме того, если s имеет вид $Exp(\,\cdot\,,\cdot\,)$, то также $s \neq u$.

Доказательство. Пункт 1 очевиден. Докажем пункт 2 при указанных ограничениях на s.

Рассмотрим сначала случай, когда u *не* имеет формы $Exp(\,\cdot\,,\cdot\,)$. Тогда i) $\ulcorner Exp(u, M)\urcorner = u$, и, следовательно, $\ulcorner M\urcorner = 1$, или ii) $\ulcorner Exp(u, M)\urcorner = Exp(u, \ulcorner M\urcorner)$ и при этом $\ulcorner M\urcorner \neq 1$. Рассмотрим оба подслучая.

В случае i) получаем $\ulcorner M'\urcorner^{\delta} = 1$. По пункту 1 уже известно, что $\ulcorner M\urcorner^{\delta} = \ulcorner M'\urcorner^{\delta} (= 1)$. Следовательно

$$\begin{aligned} \ulcorner Exp(u, M)\delta\urcorner &= \ulcorner Exp(u\delta, M\delta)\urcorner && (*)\\ &= \ulcorner Exp\big(u\delta, \ulcorner M\delta\urcorner\big)\urcorner \\ &= \ulcorner u\delta\urcorner \\ &= \ulcorner\ulcorner Exp(u, M)\urcorner\delta\urcorner. \end{aligned}$$

Здесь в $(*)$ использовано, что $Exp(u, M) \neq s$ (иначе $\ulcorner Exp(u, M)\urcorner = s$, поскольку s нормализован).

В Случае ii) положим

$$\begin{aligned} \ulcorner\ulcorner Exp(u, M)\urcorner\delta\urcorner &= \ulcorner Exp\big(u, \ulcorner M\urcorner\big)\delta\urcorner \\ &= \ulcorner Exp\big(u\delta, \ulcorner M\urcorner\delta\big)\urcorner && (*)\\ &= \ulcorner Exp\big(u\delta, \ulcorner M\urcorner\delta\big)\urcorner \\ &= \ulcorner Exp\big(u\delta, \ulcorner M\delta\urcorner\big)\urcorner && (**)\\ &= \ulcorner Exp(u\delta, M\delta)\urcorner \\ &= \ulcorner Exp(u, M)\delta\urcorner && (***) \end{aligned}$$

где в $(*)$ мы используем соотношение $Exp(u, \ulcorner M \urcorner) \neq s$ (иначе получилось бы $\ulcorner Exp(u, M) \urcorner = \ulcorner Exp(u, \ulcorner M \urcorner) \urcorner = s$); в $(**)$ ссылаемся на пункт 1 леммы; а в $(***)$ вновь задействуем условие $Exp(u, M) \neq s$. Заметим, что и в случаях (i), и в (ii) дополнительное требование $u \neq s$ (если s имеет форму $Exp(\,\cdot\,,\cdot\,)$) не требуется.

Теперь предположим, что $u = Exp(v, M')$ для некоторых v и M'. Тогда

$$\begin{aligned}
\ulcorner\ulcorner Exp(u, M)\urcorner\delta\urcorner &= \ulcorner\ulcorner Exp(v,\ M'\cdot M)\urcorner\delta\urcorner \\
&= \ulcorner Exp\big(v,\ M'\cdot M\big)\delta\urcorner && (*) \\
&= \ulcorner Exp\big(v\delta, (M'\delta\cdot M\delta\big)\urcorner && (**) \\
&= \ulcorner Exp\big(Exp(v\delta, M'\delta),\ M\delta\big)\urcorner \\
&= \ulcorner Exp(u\delta, M\delta)\urcorner && (***) \\
&= \ulcorner Exp(u, M)\delta\urcorner. && (****)
\end{aligned}$$

где $(*)$ выводится точно так же, как и в первом случае: используется то, что v не имеет формы $Exp(\,\cdot\,,\cdot\,)$ и $Exp(v, M'\cdot M) \neq s$ (иначе $\ulcorner Exp(v, M'\cdot M)\urcorner = \ulcorner Exp(u, M)\urcorner = s$). Напомним, что для первого случая предположение $v \neq s$ не требовалось. В $(**)$ вновь задействуется условие $Exp(v, M'\cdot M) \neq s$. В $(***)$ используется факт $u \neq s$ (иначе $u = s$, причём s имеет вид $Exp(\,\cdot\,,\cdot\,)$). Наконец, $(****)$ опирается на неравенство $Exp(u, M) \neq s$.

□

Лемма 3.5. Пусть σ — нормализованная замкнутая подстановка, E — множество нормализованных термов, s — нормализованный стандартный неатомарный терм, а δ — замена $[s \leftarrow 1]$. Обозначим $\sigma' = \ulcorner\sigma\delta\urcorner$. Если не существует стандартного подтерма $t \in E$ такого, что $t \sqsubseteq_\sigma s$, то $\ulcorner E\sigma'\urcorner = \ulcorner\ulcorner E\sigma\urcorner\delta\urcorner$.

Доказательство. Предположим, что не существует стандартного подтерма t множества E такого, что $t \sqsubseteq_\sigma s$. Рассмотрим множество $\Omega_s = \big\{\, t \in S(E) \mid \ulcorner t\sigma'\urcorner \neq \ulcorner\ulcorner t\sigma\urcorner\delta\big\}$.
Допустим противное, то есть $\Omega_s \neq \varnothing$. Выберем $u \in \Omega_s$ минимальным по отношению *подтерм* $\sqsubseteq$. По определению σ' терм u не может быть переменной, а так как s не атом, то u не является и константой.

Если $u = \{u_1\}^s_{u_2}$, $\{u_1\}^a_{u_2}$ или $\langle u_1, u_2\rangle$, то $\ulcorner u\sigma\urcorner = s$, то $u \sqsubseteq_\sigma s$, противоречие. Из минимальности u получаем $\ulcorner u_1\sigma'\urcorner = \ulcorner\ulcorner u_1\sigma\urcorner\delta\urcorner$ и $\ulcorner u_2\sigma'\urcorner = \ulcorner\ulcorner u_2\sigma\urcorner\delta\urcorner$, откуда $\ulcorner u\sigma'\urcorner = \ulcorner\ulcorner u\sigma\urcorner\delta\urcorner$ — противоречие с $u \in \Omega_s$.

Следовательно, остаётся единственная форма $u = Exp(u_1, M)$. Минимальность u даёт $\ulcorner v\sigma'\urcorner = \ulcorner\ulcorner v\sigma\urcorner\delta\urcorner$ для всех $v \in \mathcal{F}(u)$, и, значит,

$$Exp(\ulcorner u_1\sigma'\urcorner, \ulcorner M\sigma'\urcorner) = Exp(\ulcorner\ulcorner u\sigma\urcorner\delta\urcorner, \ulcorner\ulcorner M\sigma\urcorner\delta\urcorner).$$

Поскольку $u\sigma \neq s$ и $u_1\sigma \neq s$, из пункта 2 леммы 3.4 получаем требуемое равенство. □

Лемма 3.6. Пусть $t', t_1, \ldots, t_n, t, u$ — нормализованные стандартные термы, $z_1, \ldots, z_n \in \mathbb{Z}$, а δ — замена $[u \leftarrow 1]$ такая, что $u \neq t$ и $t = \ulcorner Exp\big(t',\, t_1^{z_1}\cdots t_n^{z_n}\big)\urcorner$. Если $t' = Exp(\,\cdot\,,\cdot\,)$, то дополнительно предполагаем $u \neq t'$. Тогда

$$\ulcorner t\delta\urcorner = \ulcorner Exp\big(\ulcorner t'\delta\urcorner, \ulcorner t'\delta\urcorner^{z_1}\cdots\ulcorner t_n\delta\urcorner^{z_n}\big)\urcorner.$$

Доказательство. Теперь предположим, что $u = Exp(v, M')$ для некоторых нормализованных v и M'. Заметим, что $v \neq Exp(\,\cdot\,,\cdot\,)$, поскольку t' нормализован. Тогда

$$\begin{aligned}
\ulcorner Exp\big(t'\delta,\, \ulcorner t_1\delta\urcorner^{z_1}\cdots\ulcorner t_n\delta\urcorner^{z_n}\big)\urcorner &= \ulcorner Exp\big(\ulcorner v\delta\urcorner,\, \ulcorner M\delta\urcorner\cdot\ulcorner t_1\delta\urcorner^{z_1}\cdots\ulcorner t_n\delta\urcorner^{z_n}\big)\urcorner && (*)\\
&= \ulcorner Exp\big(v\delta,\, M\delta\cdot(t_1\delta)^{z_1}\cdots(t_n\delta)^{z_n}\big)\urcorner\\
&= \ulcorner Exp\big(v,\, M\cdot t_1^{z_1}\cdots t_n^{z_n}\big)\delta\urcorner && (**)\\
&= \ulcorner\ulcorner Exp\big(v,\, M\cdot t_1^{z_1}\cdots t_n^{z_n}\big)\urcorner\delta\urcorner && (***)\\
&= \ulcorner t\delta\urcorner.
\end{aligned}$$

где в $(*)$ используем, что $u \neq t'$, а значит $\ulcorner t'\delta\urcorner = \ulcorner v^{\delta}\urcorner$ (при этом $\ulcorner M\delta\urcorner = 1$) или $\ulcorner t'\delta\urcorner = Exp\big(\ulcorner v\delta\urcorner, \ulcorner M\delta\urcorner\big)$. В $(**)$ задействуется условие $u \neq t$: если бы $u = Exp\big(v,\, M\cdot t_1^{z_1}\cdots t_n^{z_n}\big)$, то, поскольку u нормализован, нормализован и $Exp\big(v,\, M\cdot t_1^{z_1}\cdots t_n^{z_n}\big)$, а значит $u = Exp\big(v,\, M\cdot t_1^{z_1}\cdots t_n^{z_n}\big) = t$, что противоречит $u \neq t$. В $(***)$ используем, что $v \neq Exp(\,\cdot\,,\cdot\,)$, $u \neq t$, а также пункт 2 леммы 3.4.

Предположим теперь, что $t' \neq Exp(\,\cdot\,,\cdot\,)$. Для обеих ситуаций $u \neq t'$ и $u = t'$ рассуждения аналогичны приведённым выше: достаточно заменить v на t' и опустить $\ulcorner M\delta\urcorner$, $M\delta$ и M во всех формулах. □

Лемма 3.12. Пусть $t \in forge(E)$ и $\gamma \in forge(E)$. Предположим, что имеется вывод D_γ из E, последним шагом которого является применение правила из $\mathcal{L}_c$. Тогда существует вывод D' из E с целью t, удовлетворяющий $L_d(\gamma) \notin D'$.

Доказательство. Сначала введём некоторое обозначение. Пусть $D_1 = E_1 \to \cdots \to F_1$ и $D_2 = E_2 \to \cdots \to F_2$ — две дедукции, причём $E_2 \subseteq F_1$. Обозначим через $D = D_1 \cdot D_2$ конкатенацию шагов D_1 и D_2 (в указанном порядке); при этом из D_2 удаляются те шаги, которые выводят сообщения, уже содержащиеся в F_1, чтобы результат оставался дедукцией.

По определению дедукции правило $L_d(\gamma)$ отсутствует в D_γ. Пусть D — это D_γ без последнего шага, то есть D_γ состоит из D, за которым следует некоторое $L \in \mathcal{L}_c$. Положим $D'' = D \,.\, Deriv_t(E) = D \,.\, D'''$ где D''' получается из $Deriv_t(E)$ удалением избыточных шагов. Тогда D'' — дедукция с целью t. Рассмотрим два случая.

— Пусть $L = L_c(\gamma)$. Тогда $L_d(\gamma) \notin D''$, поскольку оба непосредственных подтерма γ были выведены уже в D. Следовательно, $D' = D''$ — искомая дедукция.

— Пусть $L = L_{oc}(\gamma)$. Если $L_d(\gamma) \notin D''$, делать больше нечего. В противном случае обозначим через F_1 конечное множество сообщений дедукции D. Из пункта (2) определения 2.11 следует, что каждый шаг из D''' вида $F_1, F_2, \gamma \longrightarrow^{L_d(\gamma)} F_1, F_2, \gamma, \beta$ можно заменить дедукцией из F_1, F_2 с целью β, в которой правило $L_d(\gamma)$ не встречается. После такой замены и последующего устранения избыточных шагов получаем требуемую дедукцию D'. □

ПРИЛОЖЕНИЕ Б

Расширение нарушителя Долева–Яо возведением в степень Диффи–Хеллмана

Лемма 4.3. Пусть E — конечное множество нормализованных стандартных сообщений, t — стандартное сообщение такое, что t выводится из E (относительно L). Пусть D — вывод из E с целью t. Тогда существует вывод D' из E с той же целью t, удовлетворяющий:

а) D' имеет ту же длину, что и D;

б) для любого DH-правила $L \in D' \cap L_o$ с головным термом t' выполнено: $t' \in E$ или существует t'-правило $L' \in D' \cap (L_d \cup L_c)$. Более того, если L — *декомпозиционное* DH-правило, то $t' \in E$ или существует t'-правило $L' \in D' \cap L_d$.

Доказательство. Пусть D — вывод из E с целью t. Построим по нему вывод D' следующим образом. Пусть $L \in D \cap L_o$ имеет вершину t' и при этом $t' \in E$, $D' \cap (L_d \cup L_c)$ не содержит t'-правил. Тогда в D найдётся правило $L' \in D \cup L_o(t')$. Пусть $L: \ t', t_1, \ldots, t_n \longrightarrow t$, $z_1, \ldots, z_n$, а $L': \ t'', t'_1, \ldots, t'_n \longrightarrow t'$, $z'_1, \ldots, z'_n$. Очевидно, $t = \ulcorner Exp\big(t'', t_1^{z_1} \cdots t_n^{z_n} {t'_1}^{z'_1} \cdots {t'_n}^{z'_n}\big) \urcorner$, и потому t может быть получен правилом $\widehat{L}: \ t'', t_1, \ldots, t_n, t'_1, \ldots, t'_n \longrightarrow t$, относящимся к множеству DH и имеющим вершину t''. Следовательно, в выводе D правило L можно заменить на $\widehat{L}$. Итеративно выполняя такую замену, получаем вывод D', удовлетворяющий условию 1, и при этом для любого $L \in D' \cap L_o$ с вершиной t' не существует предшествующего ему в D' правила $L' \in D' \cap L_o(t')$, что и даёт условие 2. Заметим, что если L является декомпозиционным правилом DH, то t' имеет форму $Exp(\cdot, \cdot)$ и, следовательно, не может быть порождён ни одним правилом из L_c. □

Лемма 4.4. Пусть $D = E_0 \to_{L_1} \ldots E_{n-1} \to_{L_n} E_n$ — вывод с целью g.

а) Предположим, что для каждого шага $E_{j-1} \to L_j E_j$ вывода D с $L_j \in \mathcal{L}_d(t)$ существует $t' \in E_{j-1}$ такое, что $t \sqsubseteq t'$ и $t' \in E_0$ или $\exists\, i < j : L_i \in \mathcal{L}_d(t')$. Тогда из $L \in D \cap \mathcal{L}_d(t)$ (для некоторого $\mathcal{L}, t$) следует $t \in \mathcal{S}(E_0)$.

б) Предположим, что для каждого $i < n$ и t с $L_i \in \mathcal{L}_c(t)$ найдётся $j > i$ такое, что L_j является t'-правилом и $t \in \mathcal{S}\big(\{t'\} \cup E_0\big)$. Тогда из $L \in D \cap \mathcal{L}_c(t)$ (для некоторого L, t) следует $t \in \mathcal{S}(E_0, g)$.

При выполнении обеих предпосылок (а) и (б) вывод D является корректным выводом с целью g.

Доказательство. а. Доказывается непосредственной индукцией по $j \in \{1, \ldots, n\}$. б. Пусть выполнены предположения пункта 2. Докажем индукцией по $n - i$, что для любого $i \in \{1, \ldots, n\}$ из $L_i \in \mathcal{L}_c(t)$ следует $t \in S(E_0, g)$. $n-i = 0$. Тогда $t = g$, а значит $t \in S(E_0, g)$. Предположения пункта а дают $j > i$ такие, что L_j — t'-правило и $t \in S(E_0, t')$. Если $L_j \in \mathcal{L}_d(t')$, то $t' \in S(E_0)$ (см. выше). Если же $L_j \in \mathcal{L}_c(t')$, то по индукционному предположению $t' \in S(E_0, g)$, а значит и $t \in S(E_0, g)$. Из предположений пунктов а и б немедленно следует, что D является корректной дедукцией с целью g. □

Лемма 4.6. Пусть $z_1, \ldots, z_n \in \mathbb{Z} \setminus \{0\}$, а $s, s_1, \ldots, s_n$ — нормализованные стандартные термы, удовлетворяющие условиям $s_i \neq s_j$ при $i \neq j$, $s_i \neq 1$ и $s_i \neq u$ для всех i, $s \neq u$, $u = \ulcorner Exp\big(s,\, s_1^{z_1} \cdots s_n^{z_n}\big) \urcorner, u = Exp(\,\cdot\,,\cdot\,)$. Пусть δ — замена $[\,u \to 2\,]$. Тогда $u = \ulcorner Exp\big(\ulcorner s\delta \urcorner,\, \ulcorner s_1\delta \urcorner^{z_1} \cdots \ulcorner s_n\delta \urcorner^{z_n}\big) \urcorner$.

Доказательство. Сначала предположим, что $s \neq Exp(\,\cdot\,,\cdot\,)$. Тогда $u = Exp(s,\, s_1^{z_1} \cdots s_n^{z_n})$. Отсюда следует, что $u \notin S(s, s_1, \ldots, s_n)$, а значит $s = s^\delta$ и $s_i = s_i^\delta$ для всех i. Следовательно, $u = \ulcorner Exp\big(\ulcorner s\delta \urcorner, \ulcorner s_1\delta \urcorner^{z_1} \cdots \ulcorner s_n\delta \urcorner^{z_n}\big)$.

Теперь предположим, что $s = Exp(v, M)$. Так как s нормализован, имеем $v \neq Exp(\,\cdot\,,\cdot\,)$. Используя, что u имеет вид $Exp(\,\cdot\,,\cdot\,)$, получаем $u = Exp\big(v, \ulcorner M \cdot s_1^{z_1} \cdots s_n^{z_n} \urcorner\big), \ulcorner M \cdot s_1^{z_1} \cdots s_n^{z_n} \urcorner \neq 1, u \notin S(v)$. Положим $E = \mathcal{F}(M) \cup \{s_1, \ldots, s_n\}$. Тогда найдутся подмножество $E' = \{\, s'_1, \ldots, s'_n\} \subseteq E$ и целые ненулевые $z'_1, \ldots, z'_n$ такие, что $u = Exp\big(v,\, {s'_1}^{z'_1} \cdots {s'_n}^{z'_n}\big), u \notin S\big(v, E'\big)$.

Утверждение. Выполняется равенство

$$M^\delta \cdot s_1^{\delta\, z_1} \cdots s_n^{\delta\, z_n} \;=\; {s'_1}^{z'_1} \cdots {s'_n}^{z'_n}.$$

Доказательство утверждения. Пусть $M = s_{n+1}^{z_{n+1}} \cdots s_{n''}^{z_{n''}}$. Определим множества индексов

$$C_i \;=\; \big\{\, j \in \{1, \ldots, n''\} \mid s_j = s'_i \big\} \quad (i = 1, \ldots, n).$$

Тогда $z'_i \;=\; \sum_{j \in C_i} z_j, \qquad C \;=\; \bigcup_{i=1}^{n'} C_i$.

$s_1^{z_1} \cdots s_n^{z_n} M \;=\; \ulcorner \prod_{i=1}^{n'} \prod_{j \in C_i} s_j^{z_j} \urcorner \;=\; \ulcorner \prod_{i=1}^{n'} {s'_i}^{z'_i} \urcorner, \ulcorner \prod_{j \notin C} s_j^{z_j} \urcorner = 1$. Так как все s_j нормализованы, получаем $\ulcorner \prod\limits_{j \notin C} s_j^{\delta\, z_j} \urcorner = \prod\limits_{j \notin C} \ulcorner s_j^{\delta z_j} \urcorner = 1$, а потому, учитывая ${s'}_i^{\delta} = {s'}_i$, равенство утверждения доказано:

$$M^{\delta}\, s_1^{\delta z_1} \cdots s_n^{\delta z_n} \;=\; {s'_1}^{z'_1} \cdots {s'_n}^{z'_n}.$$

Используя теперь $s\delta = Exp(v\delta, M\delta)$ и факты $u \neq M$, $u \notin S(v)$, $u \neq s$, получаем

$$\ulcorner Exp\big(\ulcorner s\delta \urcorner, \ulcorner s_1\delta \urcorner^{z_1} \cdots \ulcorner s_n\delta \urcorner^{z_n}\big) \urcorner = \ulcorner Exp\big(\ulcorner v\delta \urcorner, \ulcorner M\delta \urcorner \ulcorner s_1\delta \urcorner^{z_1} \cdots \ulcorner s_n\delta \urcorner^{z_n}\big) = u. \;\; \square$$

ПРИЛОЖЕНИЕ В

Правила DH допускают атаки с полиномиально ограниченными показателями произведений

Лемма 5.11. Для любого открытого сообщения или произведения t, такого что $\beta(t) = \ulcorner\beta(t)\urcorner$, выполнено $t^\beta = t$.

Доказательство. Доказательство проводится по структурной индукции по t. Если t является атомом, парой либо шифрованием, утверждение очевидно.

Пусть $t = t_1^{e_1} \cdots t_n^{e_n}$. Из свойств отображения оценки имеем: $\beta(t_i) = \ulcorner\beta(t_i)\urcorner \neq 1$ для всех i, $\beta(t_i) \neq \beta(t_j)$ при $i \neq j$, и $\beta(e_i) \neq 0$ для всех i. Отсюда непосредственно следует, что $t^\beta = t$.

Наконец, пусть $t = Exp(u, M)$. Сначала заметим, что $\ulcorner\beta(u)\urcorner \neq Exp(u', M')$ для любых нормализованных u' и M'. Действительно, иначе $\ulcorner\beta(t)\urcorner = Exp\big(\beta(u), \beta(M)\big) = Exp(u', M'') = \beta(t)$, и, следовательно, $\beta(u) = u'$. Тогда $Exp(u', M') = \ulcorner\beta(u)\urcorner = \ulcorner u'\urcorner = u'$, что противоречит нормализованности u'.

Кроме того, $\ulcorner\beta(M)\urcorner \neq 1$, поскольку иначе $Exp\big(\beta(u), \beta(M)\big) = \ulcorner\beta(t)\urcorner = \ulcorner\beta(u)\urcorner$, а мы уже знаем, что $\ulcorner\beta(u)\urcorner \neq Exp(\,\cdot\,,\cdot\,)$. Тем самым $Exp\big(\beta(u), \beta(M)\big) = \ulcorner\beta(t)\urcorner = Exp\big(\ulcorner\beta(u)\urcorner, \ulcorner\beta(M)\urcorner\big)$, и значит $\beta(u) = \ulcorner\beta(u)\urcorner$ и $\beta(M) = \ulcorner\beta(M)\urcorner$. По индукционному предположению отсюда следует $u^\beta = u$ и $M^\beta = M$. По определению t^β получаем $t^\beta = Exp(u^\beta, M^\beta) = Exp(u, M) = t$. □

Лемма 5.13. Пусть E — конечное множество открытых сообщений или произведений, такое что $S_{\text{ext}}(E) = E$, а t — максимальный (относительно упорядочения «строгий подтерм») элемент множества E. Тогда

$$\Big|\bigcup_{s\in E} S_{\text{ext}}\big(s^\beta\big)\Big|_{\text{exp}} \;\leq\; \Big|\bigcup_{s\in E\setminus\{t\}} S_{\text{ext}}\big(s^\beta\big)\Big|_{\text{exp}} + \|t\|^2_{\text{ext}}.$$

Чтобы доказать эту лемму, нам сначала нужно ограничить размер $|\cdots|_{exp}$ произведения. Это про следующее утверждение:

Утверждение 1. Для любого открытого сообщения или произведения t, такого что $t^\beta = Exp(u, M)$, выполняется

$$|M|_{\text{exp}} \;\leq\; |t| \;\cdot\; \|t\|_{\text{exp}} \;\leq\; \|t\|^2_{\text{ext}}.$$

Доказательство. Докажем индукцией по структуре t, что $|M|_{\exp} \le |t| \cdot \|t\|_{\exp}$. Так как $|t| \le \|t\|_{\text{ext}}$ и $\|t\|_{\exp} \le \|t\|_{\text{ext}}$, утверждение леммы будет следовать сразу.

Сперва положим, что $t = Exp(u', M')$ и $\beta(u') \neq Exp(\,\cdot\,,\cdot\,)$. Тогда $|M|_{\exp} \le |M'|_{\exp} \le \|t\|_{\exp}$.

Сейчас положим $t = Exp(u', M')$ и $\beta(u') = Exp(\,\cdot\,,\cdot\,)$. Пусть $u'^{\beta} = Exp(u'', M'')$. Тогда $M = (M''\cdot M')^{\beta}$ и, по индукционному предположению, $|M|_{\exp} \le |M''|_{\exp} + |M'|_{\exp} \le |u'|\,\|u'\|_{\exp} + \|t\|_{\exp} \le |t|\,\|t\|_{\exp}$, поскольку $\|u'\|_{\exp} \le \|t\|_{\exp}$ и $|u'| < |t|$.

В остальных случаях, если $t^{\beta} = Exp(u, M)$ получается для другого вида t, то существует подтерм $v \sqsubset t$ такой, что $v^{\beta} = t^{\beta}$. Неравенство тогда следует из индукционного предположения для v. □

Теперь можно приступить к доказательству Леммы 5.13:

Доказательство. Доказательство проводим, как и прежде, структурной индукцией по t. Пусть $E = S_{\text{ext}}(t)$ и обозначим $\mathcal{S}(E) = \big|\bigcup_{s\in E} S_{\text{ext}}\big(s^{\beta}\big)\big|_{\exp}$.

Если $t = \langle t_1, t_2\rangle$, то $t^{\beta} = t_1^{\beta}, t_2^{\beta}$ и $S_{\text{ext}}(t^{\beta}) \subseteq \{t^{\beta}\}\cup S_{\text{ext}}(t_1^{\beta})\cup S_{\text{ext}}(t_2^{\beta})$. Поскольку $S_{\text{ext}}(E) = E$, имеем $t_1, t_2 \in E \setminus \{t\}$. Так как $|t^{\beta}|_{\exp} = 0$, $\Big|\bigcup_{s\in E} S_{\text{ext}}(s^{\beta})\Big|_{\exp} = \Big|\bigcup_{s\in E\setminus\{t\}} S_{\text{ext}}(s^{\beta})\Big|_{\exp}$. Для случая шифрования рассуждение аналогично.

Если $t = t_1^{e_1}\cdots t_n^{e_n}$, то $S_{\text{ext}}(t^{\beta}) \subseteq \{t^{\beta}\} \cup \bigcup_i S_{\text{ext}}(t_i^{\beta})$, причём $t_1, \ldots, t_n \subseteq E \setminus \{t\}$. Следовательно, $S_{\text{ext}}(t^{\beta}) \subseteq \Big(\bigcup_{s\in E\setminus\{t\}} S_{\text{ext}}(s^{\beta})\Big) \cup \{t^{\beta}\}$. Так как $|t^{\beta}|_{\exp} \le |t|_{\exp} \le \|t\|_{\text{ext}}^2$, утверждение верно.

Пусть теперь $t = Exp(u, M)$ и $t^{\beta} = u^{\beta}$ или $t^{\beta} = u''$ или $t^{\beta} = Exp(u^{\beta}, M^{\beta})$ (см. лемму 5.10). Тогда $S_{\text{ext}}(t^{\beta}) \subseteq \big\{t^{\beta}\big\} \cup S_{\text{ext}}(u^{\beta}) \cup S_{\text{ext}}(M^{\beta})$, и опять $\Big|\bigcup_{s\in E} S_{\text{ext}}(s^{\beta})\Big|_{\exp} = \Big|\bigcup_{s\in E\setminus\{t\}} S_{\text{ext}}(s^{\beta})\Big|_{\exp}$, $\quad |t^{\beta}|_{\exp} = 0$.

Наконец, пусть $t = Exp(u, M)$, $\beta(u) = Exp(u', M')$, $u^{\beta} = Exp(u'', M'')$. Тогда $t^{\beta} = Exp\big(u'', (M''\cdot M)^{\beta}\big)$, и

$$\begin{aligned} S_{\text{ext}}(t^{\beta}) &\subseteq \{t^{\beta}\} \cup S_{\text{ext}}(u^{\beta}) \cup S_{\text{ext}}\big((M''\cdot M)^{\beta}\big) \\ &\subseteq \{t^{\beta}\} \cup \{(M''\cdot M)^{\beta}\} \cup \bigcup_{s\in E\setminus\{t\}} S_{\text{ext}}(s^{\beta}), \end{aligned}$$

где, по лемме 5.11, $S_{\text{ext}}(M''^{\beta}) = S_{\text{ext}}(M'') \subseteq S_{\text{ext}}(u^{\beta})$. Поскольку $|t^{\beta}|_{\exp} = 0$ и $|(M''\cdot M)^{\beta}|_{\exp} \le \|t\|_{\text{ext}}^2$, получаем требуемую оценку. □

Лемма 5.17. Пусть $M = t_1^{e_1} \cdots t_n^{e_n}$ и $M' = t_1'^{e_1'} \cdots t_{n'}'^{e_{n'}'}$ — два открытых произведения такие, что $\beta(t_i) = \ulcorner \beta(t_i') \urcorner$ для всех соответствующих множителей. Пусть для каждого i задан β-кортеж $(t_i^\beta, \mathcal{E}_i)$ терма t_i. Тогда пара $\Big((M' \cdot M)^\beta,\ \mathcal{E}'^{\beta}_{(M' \cdot M)} \cup \bigcup_i \mathcal{E}_i\Big)$ является β-кортежем для произведения $M' \cdot M$.

Доказательство. Пусть $t = M' \cdot M$. Очевидно, $\beta \models \mathcal{E}_t'^{\beta} \cup \bigcup_i \mathcal{E}_i$, $\quad \beta(t^\beta) = \ulcorner \beta(t) \urcorner$. Пусть $\beta' \models \mathcal{E}_t'^{\beta} \cup \bigcup_i \mathcal{E}_i$. Нужно показать, что $\ulcorner \beta'(t^\beta) \urcorner = \ulcorner \beta'(t) \urcorner$.

Утверждение I. Для любых i, j справедливо $\ulcorner \beta'(t_i) \urcorner = \ulcorner \beta'(t_i^\beta) \urcorner, \ulcorner \beta'(t_j') \urcorner = \ulcorner \beta'(t_j'^{\beta}) \urcorner$.

Доказательство утверждения 1. Из $\beta' \models \mathcal{E}_i$ сразу следует $\ulcorner \beta'(t_i) \urcorner = \ulcorner \beta'(t_i^\beta) \urcorner$. По лемме 5.11 $t_j'^{\beta} = t_j'$, следовательно $\ulcorner \beta'(t_j') \urcorner = \ulcorner \beta'(t_j'^{\beta}) \urcorner$.

Пусть классы $C_1, \ldots, C_\ell$ заданы так же, как в доказательстве леммы 5.10.

Утверждение II. Для любого k и любых $s, s' \in C_k$ выполнено $\ulcorner \beta'(s) \urcorner = \ulcorner \beta'(s') \urcorner$.

Доказательство утверждения 2. Во-первых, если $s = t_i'$ и $s' = t_j'$, то по лемме 5.11 $s^\beta = s$, $s'^{\beta} = s'$, и из определения $\mathcal{E}_t'^{\beta}$ следует $\beta'(s) = \beta'(s')$. Пусть $s = t_i$, $s' = t_j'$. Тогда $s'^{\beta} = s'$, и по определению $\mathcal{E}_t'^{\beta}$ имеем $\ulcorner \beta'(s') \urcorner = \ulcorner \beta'(s^\beta) \urcorner$. А из $\beta' \models \mathcal{E}_i$ следует $\ulcorner \beta'(s) \urcorner = \ulcorner \beta'(s^\beta) \urcorner$, откуда $\ulcorner \beta'(s') \urcorner = \ulcorner \beta'(s) \urcorner$. Аналогично рассматривается случай $s = t_i$, $s' = t_j$.

По определению $\mathcal{E}_t'^{\beta}$ для каждого $j \in J$ имеет место $\beta'(e_{C_j}) = 0$. Используя Утверждения I и II, легко заключить, что $\ulcorner \beta'(t^\beta) \urcorner = \ulcorner \beta'(t) \urcorner$. □

Лемма 5.20. Пусть $t_1, \ldots, t_n$ — открытые сообщения, s — нормализованное сообщение, β — отображение оценки, а $L \in \mathcal{L}$ — правило нарушителя такое, что $\beta(t_i) = \ulcorner \beta(t_i) \urcorner$ для всех i и $\ulcorner \beta(t_1) \urcorner, \ldots, \ulcorner \beta(t_n) \urcorner \ \to\ s \in L$. Тогда существует открытое сообщение t, система линейных уравнений $\mathcal{E}$ и расширение β отображения β такие, что

(1) $\beta(t) = s$;
(2) $\beta \models \mathcal{E}$;
(3) $\ulcorner \beta'(t_1) \urcorner, \ldots, \ulcorner \beta'(t_n) \urcorner \ \to\ \ulcorner \beta'(t) \urcorner$ для всякого $\beta' \models \mathcal{E}$;
(4) $\max\big\{|e| \ \big|\ e \in \mathcal{L}_{\exp}(t)\big\} \ \le\ \max\big\{|e| \ \big|\ e \in \mathcal{L}_{\exp}(t_1, \ldots, t_n)\big\} + n$;
(5) размер $\mathcal{E}$ полиномиально ограничен величиной $\|t_1, \ldots, t_n\|_{\text{ext}}$.

Чтобы доказать лемму, сначала докажем следующее утверждение:

Утверждение. Пусть $t_0, \dots, t_n$ — открытые сообщения и β — отображение оценки, такое что $\beta(t_i) = \ulcorner\beta(t_i)\urcorner$ для всех i. Пусть $z_1, \dots, z_n$ — целочисленные переменные, не встречающиеся в термах t_i. Обозначим $M = t_1^{z_1} \cdots t_n^{z_n}$, $t = Exp\big(t_0, M\big)^\beta$. Тогда каждый коэффициент в линейных уравнениях, появляющихся в t, не превосходит $\max\big\{|e| \;\big|\; e \in \mathcal{L}_{\exp}(t_0, t_1, \dots, t_n)\big\} + n$.

Доказательство. По лемме 5.11 все $t_i^\beta = t_i$. Рассмотрим два случая.

Пусть $\beta(t_0) = \ulcorner\beta(t_0)\urcorner \neq Exp(\,\cdot\,,\cdot\,)$. Тогда $t = Exp(t_0, M)^\beta$ не вносит новых показателей, и утверждение очевидно.

Пусть $\beta(t_0) = \ulcorner\beta t_0 = Exp(u', M')$, т. е. $t_0 = Exp(u'', M'')$ для некоторых u'', M'' с $\beta(u'') = u'$ и $\beta(M'') = M'$. Если $t = u''$, то новые показатели отсутствуют и предельная оценка выполняется тривиально. Иначе $t = Exp\big(u'',\, (M'' \cdot M)^\beta\big)$, $(M'' \cdot M)^\beta \neq 1$. Пусть $M'' = t_1''^{e_1''} \cdots t_n''^{e_n''}$. По условию $\beta(t_i'') = \ulcorner\beta(t_i'')\urcorner$ при всех i, и все $\beta(t_i'')$ попарно различны. Разобьём индексы на классы эквивалентности $C_1, \dots, C_\ell$, как в доказательстве леммы 5.10. Тогда $t = \prod_{j \notin J \cup \{1\}} \big(s_{C_j}^\beta\big)^{e_{C_j}}$, где в каждом классе C_j есть ровно один представитель вида t_i'' или t_i. Поэтому для каждого j $|e_{C_j}|$ не превосходит $\max\{|e| \mid e \in L_{\exp}(t_0, t_1, \dots, t_n)\} + n$. Остальные подтермы t лежат внутри некоторых t_i, и для них оценка задана индукционным предположением. Это завершает доказательство утверждения. □

Теперь докажем Лемму 5.20:

Доказательство. Рассмотрим случаи в зависимости от правила нарушителя L.

Пусть $L = L_{p1}$. Тогда $n = 1$, $\ulcorner\beta(t_1)\urcorner = \langle a, b\rangle$, $s = a$, $t_1 = \langle a', b'\rangle$, где a, b — нормализованные сообщения, a', b' — открытые сообщения, $\beta(a') = a$, $\beta(b') = b$. Положим $t = a'$, $\mathcal{E} = \varnothing$, расширения β не требуются. Ясно, что условия (1)–(5) выполнены. Аналогичные рассуждения работают для L_{p2}, L_{ad} и L_c.

Теперь положим, что$L = L_{sd}$. Тогда $n = 2$, $\ulcorner\beta(t_1)\urcorner = \{a\}_s^b$, $\ulcorner\beta(t_2)\urcorner = b$ для нормализованных a, b. Значит, $t_1 = \{a'\}_s^b, t_2 = b''$, где a', b', b'' — открытые сообщения с $\beta(a') = a$, $\beta(b') = \beta(b'') = b$. Положим $t = a', \mathcal{E} = \mathcal{E}_{b,b}^\beta$, расширения β не вносятся. По лемме 5.5 проверяется, что условия (1)–(5) выполняются.

Наконец, положим, что $L = L_o$. Тогда $s = \ulcorner Exp\big(\beta(t_1),\, \beta(t_2)^{a_2} \cdots \beta(t_n)^{a_n}\big)\urcorner, a_i \in \mathbb{Z}$. Определим новые переменные $z_2, \ldots, z_n$ и терм $t = Exp\big(t_1,\, t_2^{z_2} \cdots t_n^{z_n}\big)^{\beta}, \mathcal{E} = \mathcal{E}_t^{\beta}$, расширив β так, что $\beta(z_i) = a_i$ для всех i. По лемме 5.10 имеем $s = \ulcorner \beta\big(Exp(t_1, t_2^{z_2} \cdots t_n^{z_n})\big)\urcorner = \beta(t), \beta \models \mathcal{E}$, а для любого $\beta' \models \mathcal{E}$ $\ulcorner \beta'(t)\urcorner = \ulcorner \beta'\Big(Exp(t_1, t_2^{z_2} \cdots t_n^{z_n})\Big)\urcorner = \ulcorner Exp\big(\beta'(t_1),\, \beta'(t_2)^{\beta(z_2)} \cdots \beta'(t_n)^{\beta(z_n)}\big)\urcorner$. Утверждение о полиномиальном ограничении показателей даёт условие (4), а из леммы 5.18 вытекает условие (5). $\square$