Московский Физико-Технический Институт (Национальный исследовательский университет)
Кафедра защиты информации

Дисциплина: «Защита информации»

КУРСОВАЯ РАБОТА (Эссе)

Возможности и пределы обеспечения стойкости бесконтактных систем к релейным атакам на основе доказательств с нулевым разглашением

Выполнил: Тулупов Н. Д., Б01-204
Проверила: Мозолина Н.В.

Долгопрудный 2025

Contents

Аннотация

Бесконтактные системы (RFID/NFC, EMV, PKES) уязвимы к релейным атакам, поскольку классические ZK/PoK-протоколы подтверждают знание секрета, но не контролируют близость устройства. Цель работы — определить границы применимости ZK и обосновать, когда необходимо дополнять его протоколами дистанционного ограничения (distance-bounding) и/или UWB-дальнометрированием. Показано, что «чистое» ZK не обеспечивает стойкость к relay; сформулированы практические рекомендации и ориентиры по параметрам DB для типовых сценариев (NFC-пропуска, EMV, PKES).

Ключевые слова: zero-knowledge, relay attack, distance-bounding, NFC, UWB, EMV.

Введение

Бесконтактные системы (RFID/NFC-карты, платежные приложения, автомобильные PKES и т. п.) широко применяются, однако уязвимы к *релейным атакам* (relay), при которых противник прозрачно ретранслирует легитимные сообщения между проверяющим и токеном, не нарушая криптографию. Классические протоколы аутентификации, в том числе основанные на доказательствах с нулевым разглашением (ZK/PoK), подтверждают *знание секрета*, но не контролируют *близость* устройства к считывателю, поэтому сами по себе не гарантируют стойкость к relay [1], [2], [3], [4].

Объект исследования: бесконтактные аутентификационные системы (RFID/NFC, EMV contactless, PKES).

Предмет исследования: криптографические и физические методы обеспечения устойчивости к релейным атакам (ZK/PoK, протоколы дистанционного ограничения Distance-Bounding, UWB ToF).

Цель работы: определить, в каких условиях аутентификация на основе ZK/PoK достаточна для противодействия релейным атакам, а где необходимо дополнять её протоколами дистанционного ограничения (DB) и/или безопасным дальнеметрированием UWB; сформулировать практические рекомендации по выбору подхода для типовых сценариев.

Практическая значимость: полученные правила выбора («ZK» vs «ZK+DB» vs «UWB») и ориентиры по параметрам DB (минимально необходимое k под заданный уровень риска) позволяют проектировать бесконтактные системы со встроенной стойкостью к relay без ухудшения UX

1 Доказательства с нулевым разглашением

1.1 Определение и свойства

Доказательство с нулевым разглашением (Zero-Knowledge, ZK) — интерактивный протокол между доказывающим P и проверяющим V, в котором V убеждается в истинности утверждения, не узнавая о секрете ничего сверх факта истинности [1], [5], [6]. Базовые свойства: полнота (честный P убеждает честного V для верных утверждений), корректность (обманщик не убеждает V, кроме как с пренебрежимо малой вероятностью) и нулевое разглашение. Для аутентификации используют доказательства знания (PoK), где успешность протокола имплицирует обладание конкретным секретом (существует экстрактор) [5]. На практике применяются Σ-протоколы (шаблон commit-challenge-response) [2] и стандартизованные варианты (например, ISO/IEC 9798-5 [3]).

Для объяснения принципа работы ZK рассмотрим интуитивный пример: “пещера Пегги и Виктора ”[7] (см. рис. 1). Доказывающий (Peggy) заходит в кольцевую пещеру и фиксируется на одной из веток (коммит). Затем проверяющий (Victor) случайно кричит: "Выйди слева/справа!" (вызов). Если у доказывающего есть пароль к потайной двери, он всегда выполнит требование (ответ). Без пароля он угадывает верно лишь с вероятностью $1/2$ за раунд; повторение раундов экспоненциально снижает шанс обмана (для 20 повторов — вероятность обмана 10^{-6}).

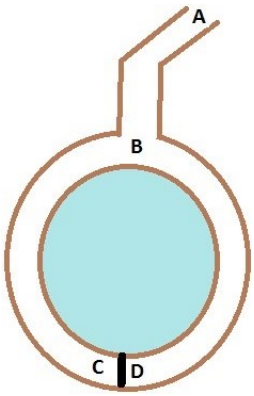

Figure 1: Иллюстрация к примеру

1.2 Пример ZK-аутентификатора: протокол Feige-Fiat-Shamir (FFS) [2]

Пусть доверенный центр генерирует два больших простых числа p и q и публикует их произведение $n = pq$ (факторы p и q остаются секретными). Секрет пользователя s выбирается взаимно простым с n, открытый ключ определяется как $v \equiv s^2 \pmod{n}$. Один раунд протокола:

a) **Commit:** выбрать случайный r и отправить $x \equiv r^2 \pmod{n}$;
b) **Challenge:** проверяющий выбирает бит $e \in \{0, 1\}$;
c) **Response:** отправить $y \equiv r\, s^e \pmod{n}$;
d) **Verify:** принять, если $y^2 \equiv x\, v^e \pmod{n}$.

Зная s, доказывающий проходит любой вызов; не зная секрета, он отвечает правильно лишь с вероятностью $1/2$. По двум успешным ответам на один и тот же коммит с разными вызовами ($e = 0$ и $e = 1$) секрет извлекается как $s \equiv y_1\, y_0^{-1} \pmod{n}$ — это формализует *доказательство знания* [2], [8].

Для честного проверяющего протокол обладает свойством нулевого разглашения: можно, выбирая случайные (e, y) и полагая $x \equiv y^2 v^{-e} \pmod{n}$, сгенерировать стенограммы, неотличимые от реального взаимодействия [2], [8].

1.3 Использование и уязвимость ZK

ZK/PoK удобны для конфиденциальной аутентификации токенов (карты/брелоки/смарт-метки) и клиентов мобильных кошельков: секрет остаётся в устройстве, подтверждается лишь *факт владения* (см. механизмов ISO/IEC 9798-5 [3]). ZK-протоколы просты по вычислениям и хорошо вписываются в ограниченные платформы (аппаратура, смарт-карты, защищённые элементы/TEE).

Однако у таких алгоритмов существует серьезный недостаток. ZK и PoK отвечают на вопрос *кто ты* (знаешь ли секрет), но не отвечают на вопрос *где ты*. В транскрипте нет измерения времени пролёта сигнала (ToF), то есть отсутствует привязка к расстоянию между P и V. Злоумышленник, выступая *релеем*, может прозрачно пересылать сообщения x, e, y, и все криптографические равенства сохранятся. Следовательно, сами по себе ZK-протоколы не обеспечивают стойкость к *relay* и требуют дополнения механизмами, контролирующими задержку/расстояние [9], [10], [11].

2 Релейные атаки

2.1 Определение и предпосылки

Релейная атака (relay) — это класс атак, при которых противник прозрачно пересылает (ретранслирует) легитимные сообщения между честным проверяющим V и честным доказывающим (токеном/смарт-картой) P, не нарушая криптографические механизмы протокола. Если протокол аутентификации не привязан к времени пролёта сигнала (time of flight, ToF), то проверяющий не отличит взаимодействие «вблизи» от взаимодействия через длинный канал, и аутентификация пройдёт успешно [4], [10].

Практические предпосылки успеха:

- **Нет измерения ToF** или допустимое окно задержек слишком широкое [4];
- **Физически удлинимый канал**: злоумышленник может построить «туннель» (провод, Wi-Fi/сотовая связь, сверхрегенеративные ретрансляторы и т. п.);
- **Слоистая ретрансляция**: возможна как «глухая» аналоговая (amplify-and-forward), так и цифровая с демодуляцией/повторной модуляцией или даже протокольная relay на более высоких уровнях стека [4].

2.2 Основные виды релейных атак

Атака мафии (mafia fraud) — классический сценарий «двух жуликов». Один нападающий (*ghost*) у проверяющего притворяется картой; второй (*leech*) рядом с владельцем перехватывает/передаёт ответы настоящей карты. Они туннелируют запросы и ответы так быстро, как позволяет среда. Криптографические проверки сходятся, и V «верит», что общается с настоящим токеном [4], [10].

Рассмотрим пример PKES — бесключевой доступ к автомобилю (см. рис. 2). Автомобиль (V) будит ключ на частоте ∼125 kHz (LF) и ждёт ответ на UHF (например, 433/868 MHz). Злоумышленник A у машины ретранслирует LF-вызов к B по туннелю. Напарник B у владельца доставляет вызов настоящему ключу, ключ (жертва) формирует ответ, B возвращает UHF-ответ по каналу назад на A, тот - на машину. Машина принимает корректный ответ и открывается/заводится — хотя легитимный ключ физически далеко [11].

Атака террористов (terrorist fraud) — усложнённый вариант «мафии»: владелец токена *сознательно* помогает нападающему, но хочет не раскрывать свой секрет полностью (например, даёт однократно используемую подсказку/вспомогательные данные). Такая модель важна при оценке DB-протоколов: защищаются ли они, даже если токен частично сотрудничает с атакующим [4], [12]. Ещё один вид релейной атаки — **distance fraud**. В данном случае сам токен пытается *имитировать близость*

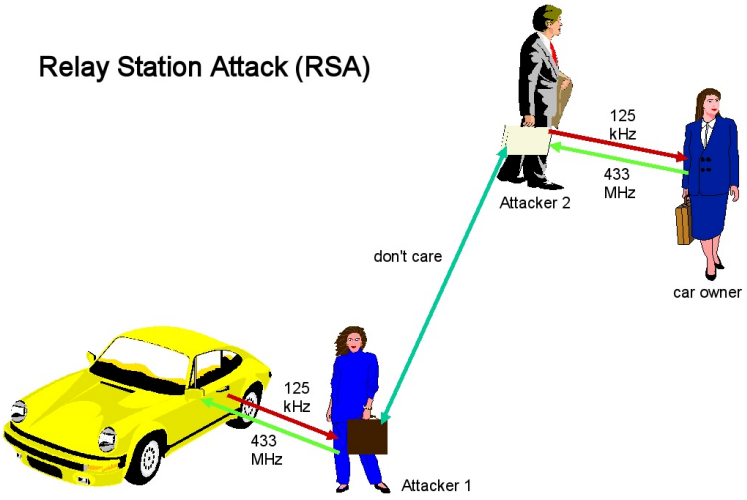

Figure 2: Атака мафии на примере бесключевого доступа к автомобилю

(например, заранее угадывать биты ответа в DB-раундах) [4], [13].

Классической аутентификации (включая ZK) не хватает одного ключевого свойства — привязки к расстоянию. Проверяющему нужно каким-то образом оценивать верхнюю границу d на дистанцию до токена по измеренной задержке сигнала. Соответственно, естественное развитие ZK-протоколов — дополнение их фазой дистанционного ограничения: верификатор измеряет время пролёта коротких запросов и ответов, так что любой «длинный» туннель неизбежно вносит дополнительную задержку, которая фиксируется и приводит к отклонению сеанса [4], [12], [13].

3 Протоколы дистанционного ограничения (distance-bounding)

3.1 Идея

Distance-bounding (DB) добавляет к аутентификации измерение *времени пролёта* сигнала (time of flight, ToF). Верификатор V запускает серию очень коротких раундов «вызов→ответ», где обработка на токене P сведена к простейшей операции (выбор заранее подготовленного бита). Если измеренная круговая задержка t_{round} мала, то верхняя граница расстояния

$$d \;\le\; \frac{c}{2}\,(t_{\text{round}} - \delta_{\text{proc}})$$

достаточно мала, чтобы считать P «рядом». Здесь c — скорость света, δ_{proc} — строго ограниченная задержка обработки на токене. Релейная атака добавляет ненулевое *туннельное* запаздывание, из-за чего ответы приходят позже дедлайна и отклоняются. Классический обзор DB-протоколов см. [4], исходная идея описана также в [13]

3.2 Два базовых протокола: Brands–Chaum и Hancke–Kuhn

Brands–Chaum (BC). Классический DB-протокол [13]. До «быстрой» фазы стороны подготавливают секретные последовательности $\alpha = (\alpha_1, \ldots, \alpha_k)$ и $\beta = (\beta_1, \ldots, \beta_k)$ (обычно с коммитом). Затем выполняются k мгновенных раундов: на i-м раунде V посылает бит α_i, а P *немедленно* отвечает соответствующим битом β_i (или простой функцией от α_i и локального секрета — в зависимости от варианта). V проверяет, что ответы приходят в пределах жёстко заданных временных ограничений; после быстрой фазы P отправляет «медленное» доказательство знания/целостности подготовленных значений, связывая результат с долгой аутентификацией. Вероятность успешного обмана «мафией» (mafia fraud) у чистого BC равна 2^{-k} (в каждом раунде атакующий угадывает

корректный бит с вероятностью 1/2, раунды считаются независимыми) [4], [13]. Схема быстрой фазы показана на рис.3.

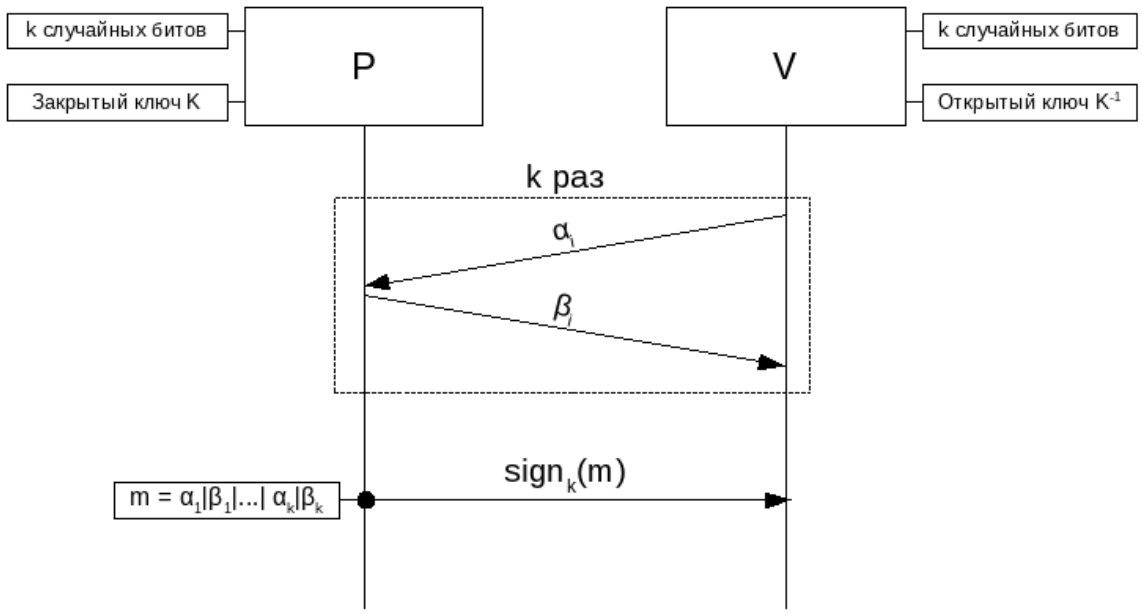

Figure 3: Схема быстрой фазы протокола Brands-Chaum.

Hancke–Kuhn (HK). Практически ориентированный протокол, спроектированный для RFID/NFC-систем [12]. V генерирует одноразовый ключ N_V и по псевдослучайной функции $h(k, N_V)$ получает пары битовых векторов (R^0, R^1) длины k. В быстрой фазе V посылает случайные челленджи $c_i \in \{0, 1\}$, а P *мгновенно* отвечает $R_i^{c_i}$. V проверяет совпадение и тайминги. См. схему на рис.4. Для атаки «мафии» оптимальная стратегия (предзапрос одного из двух возможных ответов и угадывание при неверном c_i) даёт верхнюю оценку вероятности успеха $(\frac{3}{4})^k$ [4], [12]. Параллельно анализируются и другие метрики: *distance fraud* (сам токен пытается казаться ближе) и *terrorist fraud* (владелец помогает атакующему); их границы зависят от варианта HK и модели канала. Существуют также усовершенствованные варианты, например Swiss-Knife, которые повышают стойкость к всем трём типам атак и лучше переносят ошибки канала [14]; подробный разбор этих схем выходит за рамки данной работы.

3.3 Оценки вероятностей успеха для mafia-fraud

Пусть в быстрой фазе k раундов.

- Для BC: $\Pr[\text{успех}] = 2^{-k}$ [4], [13].
  Например, $k = 32 \Rightarrow 2^{-32} \approx 2.3 \cdot 10^{-10}$; $k = 64 \Rightarrow 2^{-64} \approx 5.4 \cdot 10^{-20}$.
- Для HK (верхняя граница): $\Pr[\text{успех}] \leq \left(\frac{3}{4}\right)^k$ [4], [12].
  Например, $k = 32 \Rightarrow (3/4)^{32} \approx 1.0 \cdot 10^{-4}$; $k = 64 \Rightarrow (3/4)^{64} \approx 1.0 \cdot 10^{-8}$.

Эти оценки предполагают жёстко фиксированные временные ограничения на ответы (без джиттера и неопределённости), а также отсутствие раннего обнаружения и позднего коммита со стороны атакующего сверх принятых в модели ограничений. На практике значение k выбирают исходя из требуемого уровня риска, максимально допустимой длительности быстрой фазы и ограничений по энергопотреблению устройства, а также с учётом ошибок канала (false reject/false accept) [4].

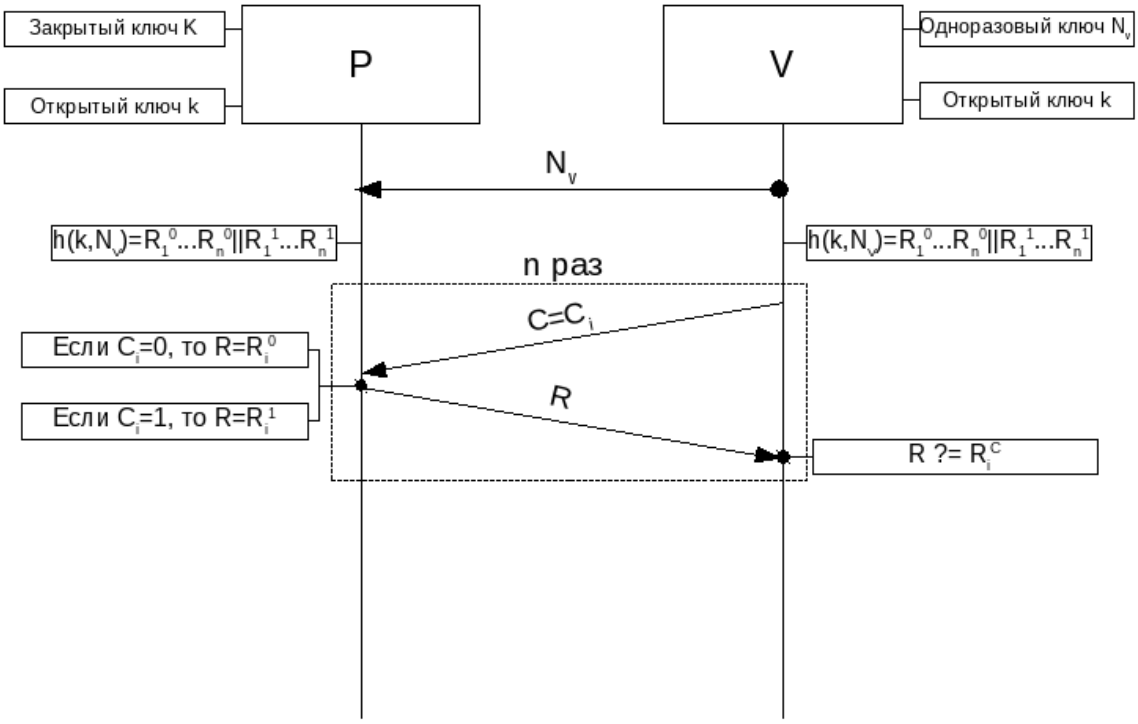

Figure 4: Схема быстрой фазы протокола Hancke-Kuhn.

3.4 Применение в NFC/PKES/UWB и композиция с аутентификацией

- **RFID/NFC и пропускные системы.** DB-фаза проводится до или совместно с логической аутентификацией (например, PoK/ZK). Быстрая фаза реализуется на низком уровне, чтобы δ_{proc} была фиксированной и минимальной; «медленная» фаза криптографически связывает результат DB с идентичностью токена (напр., MAC/NIZK поверх стенограммы быстрой фазы) [4], [15].
- **PKES (авто).** Классические LF+UHF-схемы уязвимы к relay; современная практика — *безопасное дальнометрирование на UWB*: IEEE 802.15.4z (HRP) со взаимной аутентификацией и проверкой ToF, профили FiRa для межоперабельности смартфон↔авто/брелок [16], [17]. Это физическая реализация идеи DB (импульсная радиосвязь + точный ToF) с криптографической привязкой кадров.
- **Композиция «ZK + DB».** ZK/PoK отвечает на *кто ты*, DB — на *где ты*. На практике их комбинируют: (i) «быстрая» DB-фаза ограничивает расстояние, (ii) «медленная» аутентификация (например, ZK по ISO/IEC 9798-5) привязывает результат DB к субъекту и снижает риск подмены [4].

Итог: DB или UWB-ranging необходимы для стойкости к relay; ZK остаётся корректным механизмом идентификации и приватности, но *не заменяет* контроль расстояния.

Таким образом, в главах 2–4 последовательно были рассмотрены (i) свойства ZK/PoK, (ii) модели релейных атак и (iii) протоколы дистанционного ограничения и их применение в NFC/PKES/UWB. Эти результаты используются в заключении, где суммируются основные выводы и формулируются практические рекомендации по выбору подхода («ZK», «ZK+DB» или «UWB») для типовых сценариев.

Заключение

Опираясь на рассмотренные модели релейных атак и протоколы дистанционного ограничения, в работе определены границы применимости ZK и условия необходимости DB/UWB. Показано, что **ZK/PoK не обеспечивает стойкость к relay** без контроля времени пролёта; DB добавляет привязку к расстоянию. Для мафиозной атаки приведены следующие ориентиры на вероятность успеха: *Brands–Chaum* — $\Pr \leq 2^{-k}$ (достаточно $k \approx 20$ для риска 10^{-6}), *Hancke–Kuhn* — $\Pr \leq (3/4)^k$ (нужно $k \approx 48$) [4], [12], [13].

В качестве практических рекомендаций можно выделить следующее: NFC-пропуска целесообразно реализовывать по схеме **ZK+DB**; для PKES актуален переход на **UWB secure ranging** (IEEE 802.15.4z/FiRa); в случае EMV важны усиление политиками противодействия релейным атакам и, при возможности, использование UWB. Сформулированные ориентиры по выбору схемы и по параметру k позволяют проектировать системы под заданный уровень риска.

Вместе с тем у рассматриваемого подхода есть ограничения: DB чувствителен к джиттеру и аппаратным задержкам, а в реальных каналах необходимо закладывать запас на ошибки. В качестве перспективных направлений развития можно отметить помехоустойчивые варианты DB-протоколов и более тесную композицию NIZK с DB/UWB.

References

[1] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," in *Proceedings of the 17th ACM Symposium on Theory of Computing (STOC'85)*, ACM, 1985, pp. 291–304. DOI: 10.1145/22145.22178.

[2] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Advances in Cryptology — CRYPTO '86*, A. M. Odlyzko, Ed., ser. Lecture Notes in Computer Science, vol. 263, Berlin, Heidelberg: Springer, 1987, pp. 186–194, ISBN: 978-3-540-18047-0. DOI: 10.1007/3-540-47721-7_12.

[3] *Information technology — security techniques — entity authentication — part 5: Mechanisms using zero-knowledge techniques*, Geneva, Switzerland: International Organization for Standardization, 2009.

[4] G. Avoine, M. A. Bingöl, I. Boureanu, V. Iovino, and T. Yalçın, "Security of distance-bounding: A survey," *ACM Computing Surveys*, vol. 51, no. 5, 94:1–94:33, 2018. DOI: 10.1145/3264628.

[5] O. Goldreich, S. Micali, and A. Wigderson, "Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems," in *Proceedings of the 27th Annual Symposium on Foundations of Computer Science (FOCS'86)*, IEEE Computer Society, 1986, pp. 174–187. DOI: 10.1109/SFCS.1986.25.

[6] F. Hao, *Schnorr non-interactive zero-knowledge proof*, RFC 8235, Sep. 2017. DOI: 10.17487/RFC8235.

[7] J.-J. Quisquater, M. Quisquater, M. Quisquater, M. Quisquater, L. C. Guillou, M.-A. Guillou, G. Guillou, A. Guillou, G. Guillou, and S. Guillou, "How to explain zero-knowledge protocols to your children," in *Advances in Cryptology — CRYPTO '89: 9th Annual International Cryptology Conference, Santa Barbara, August 20–24, 1989, Proceedings*, G. Brassard, Ed., ser. Lecture Notes in Computer Science, Rus. exposition: «Как объяснить протокол доказательства с нулевым разглашением вашим детям», vol. 435, Berlin; Heidelberg; New York: Springer, 1990, pp. 628–631, ISBN: 978-0-387-97317-3. DOI: 10.1007/0-387-34805-0_60.

[8] U. Feige, A. Fiat, and A. Shamir, "Zero-knowledge proofs of identity," *Journal of Cryptology*, vol. 1, no. 2, pp. 77–94, 1988, ISSN: 0933-2790. DOI: 10.1007/BF02351717.

[9] G. Avoine, M. A. Bingöl, I. Boureanu, V. Iovino, and T. Yalçın, "Security of distance-bounding: A survey," *ACM Computing Surveys*, vol. 51, no. 5, 94:1–94:33, 2018. DOI: 10.1145/3264628.

[10] Z. Kfir and A. Wool, "Picking virtual pockets using relay attacks on contactless smartcard systems," in *SecureComm 2005: First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, IEEE, 2005, pp. 47–58. DOI: 10.1109/SECURECOMM.2005.32.

[11] A. Francillon, B. Danev, and S. Čapkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, Internet Society, 2011.

[12] G. P. Hancke and M. G. Kuhn, "An rfid distance bounding protocol," in *SecureComm 2005: 1st Int. Conf. on Security and Privacy for Emerging Areas in Communications Networks*, IEEE, 2005, pp. 67–73. DOI: 10.1109/SECURECOMM.2005.56.

[13] S. Brands and D. Chaum, "Distance-bounding protocols," in *Advances in Cryptology — EUROCRYPT '93*, ser. Lecture Notes in Computer Science, vol. 765, Springer, 1994, pp. 344–359. DOI: 10.1007/3-540-48285-7_30.

[14] C. H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, and O. Pereira, "The swiss-knife rfid distance bounding protocol," in *Information Security and Cryptology — ICISC 2008*, ser. Lecture Notes in Computer Science, vol. 5461, Springer, 2009, pp. 98–115. DOI: 10.1007/978-3-642-00730-9_7.

[15] D. Singelee and B. Preneel, "Location verification using secure distance-bounding protocols," in *Proceedings of the 2005 IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS 2005)*, IEEE, 2005, ISBN: 978-0-7803-9465-0.

[16] *Ieee standard for low-rate wireless networks — amendment 1: Enhanced ultra wideband (uwb) physical layers (phys) and associated ranging techniques*, IEEE, 2020.

[17] FiRa Consortium, "Uwb secure ranging in fira," FiRa Consortium, Tech. Rep., 2022.