Opinion: Distance Bounding Under Different Assumptions

David Gerault
david@gerault.net
Nanyang Technological University, Singapore

Ioana Boureanu
i.boureanu@surrey.ac.uk
University of Surrey, UK

ABSTRACT

Distance-bounding protocols were introduced in 1993 as a countermeasure to relay attacks, in which an adversary fraudulently forwards the communication between a verifier and a distant prover. In the more than 40 different protocols that followed, assumptions were taken on the structure of distance-bounding protocols and their threat models. In this paper, we survey works disrupting these assumptions, and discuss the remaining challenges.

CCS CONCEPTS

• **Security and privacy → Authentication**; **Security protocols**; *Formal security models*; Cryptanalysis and other attacks; • **Networks** → *Mobile and wireless security*.

ACM Reference Format:
David Gerault and Ioana Boureanu. 2019. Opinion: Distance Bounding Under Different Assumptions. In *12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19), May 15–17, 2019, Miami, FL, USA.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3317549.3319729

1 INTRODUCTION

In relay attacks, an adversary forwards back and forth the communications between a a verifier (e.g., an RFID reader) and a prover (e.g., an RFID card) found outside the verifier's range; the adversary does this in a fraudulent manner, in order to gain illicit access to a service. Distance-bounding (DB) protocols were introduced by Brands and Chaum in 1993 to counteract relay attacks. In these protocols a verifier measures the round-trip times (RTTs) of its exchanges with a prover, to estimate the distance between the two; if the RTTs are greater than a certain threshold, then relay attacks are probable and the verifier rejects the transaction. Relay attacks against contactless payments [36] triggered Mastercard to add relay protection through distance bounding [20]; so, after 25 years of research, distance bounding is finally adopted by the industry.

The threats [4] considered in "academic" distance bounding are:

Mafia Fraud (MF). Two collaborating adversaries impersonate a distant prover in front of a verifier. Typically, one of the adversaries presents a fake verifier to the victim prover, while the other presents a fake prover to the legitimate verifier.

Distance Fraud (DF). A distant dishonest prover authenticates from afar by misleading the verifier in its measurements.

Distance Hijacking (DH). Distance hijacking is a generalisation of distance fraud; in a DF, no prover is close to the verifier, whereas in a DH, honest provers are to be found close to the verifier.

Terrorist Fraud (TF). A distant prover, helped by an accomplice located close to the verifier, tries to authenticate. To exclude trivial attacks where the prover gives his secret key to his accomplice, the fraud is considered successful only if the accomplice cannot authenticate on his own, once the prover no longer helps him.

A wide range of variations of these attacks have appeared, e.g., see [14]. Indeed, the threat model for DB is in constant evolution [23], and new attacks appear regularly: [4, 11] present more than 40 protocols, most of which are vulnerable to at least one attack. In particular, the notion of terrorist fraud and how to provably resist it lead to numerous publications, *e.g.*, [5, 21, 24, 39].

Contributions.
1. We critically survey works that, in a quest for better results, have challenged the well-established assumptions in distance-bounding.
2. We discuss what could be achieved by lifting more assumptions.

2 DISRUPTING CLASSICAL ASSUMPTIONS

The main assumptions for academic distance-bounding protocols were introduced in [10] and further extended in [15]. They are mostly related to physical-layer constraints to obtain reliable time measurements. Following these assumptions, most protocols are divided in two: a). a phase which is not time-critical and bares hardly any restrictions; b) a timed phase, in which 1-bit messages are exchanged and no expensive computation can be is performed. This section surveys approaches that bypass traditional assumptions.

Assumption 1: Single-bit challenges and responses. During the timed phases, only single-bit messages should be exchanged.

This assumption has been widely adopted in most academic distance-bounding protocols, except for a few exceptions, such as [31]. The assumption is however challenged by practical implementations: new relay-counteractions by 3DB [16], Mastercard's relay resistance protocol [20] and NXP's distance-bounding protocol [37]. These practical protocols share a similar design: during the timed phase, the verifier sends a bitstring nonce and the prover replies with another bitstring nonce. Afterwards, the prover sends a message authenticating the transcript (including both nonces), either via a signature or a MAC.

Assumption 2: Error tolerance. Distance-bounding protocols must account for the bit errors that occur during the timed phases.

Tolerance of transmission-errors is typically provided by granting authentication even if not all responses are correct, but no more than a given proportion/number are incorrect. Yet, enforcing such tolerances generally lowers DB security. For instance, the DB3 protocol [24] with noise tolerance generally requires 43 rounds for a security-level equivalent to 20 rounds of its noiseless version. Moreover, it was shown that noise-tolerance lead to terrorist frauds on some protocols that were otherwise secure [22].

WiSec '19, May 15–17, 2019, Miami, FL, USA

ACM ISBN 978-1-4503-6726-4/19/05…$15.00
https://doi.org/10.1145/3317549.3319729

Moreover, the need for error tolerance was traditionally argued in relation to specific physical implementations and 1-bit messages. Yet, the new bit-encoding used in the distance-bounding system proposed by 3DB [16] eliminates transmission errors, and their physical layer securely uses multiple-bit challenges and responses [35].

Assumption 3: Honest Verifiers. The verifiers are always honest.

Traditional computational formal models [9, 19] exclude malicious verifiers. Yet, in contactless payments for instance, the verifiers should be considered (at least in part) dishonest – as malware-infected payment terminals exist [32]. Indeed, recent Dolev-Yao [18]-based models for formal verification [14, 17, 29] as well as cryptographic formalisms [26] relax this assumption. And, indeed, considering dishonest verifiers lead to new attacks [29] on otherwise-secure protocols such as TREAD [5].

Assumption 4: Broadcast messages. Messages are broadcast and can all be read by DB-driven adversaries.

On the one hand, this assumption can be bypassed through the use of directional antennas [2]. On the other, leveraging this possibility, Ahmadi et al. [2] exhibit terrorist frauds against existing protocols, which were otherwise secure.

Assumption 5: Unilateral (Fixed) Timing. Challenges are sent at fixed time intervals. Only verifiers measure time, provers do not.

First, there are no more than 4 protocols [6, 12] in the vast DB literature in which both parties mutually verify their relative distance. Second, in the first DB paper [10], the idea of the verifier sending the challenges at varying intervals was mentioned. This was revisited in [27]. To this end, [27] proposes two main extensions to the DBopt protocols [24]: 1). the prover measures the time at which it received a challenge; 2) the verifier sends challenges at randomised intervals. Third, randomised challenge-sending intervals improve resistance to distance fraud [24]: if a prover sends his response before receiving the challenge, he cannot be sure his response will arrive after the challenge is issued. And, adding time-measurements by the prover and including them in the final authenticated message improves mafia-fraud resistance [24]. Using both strategies together allows to significantly reduce the number of rounds required for the DBopt protocols to be secure.

Assumption 6: Relevance of Terrorist Fraud. Many discussed provable terrorist-fraud resistance: *e.g.* [5, 9, 21, 39].

Yet, provable terrorist-fraud resistance typically lowers the overall security of the protocols [24]. The relevance of terrorist-fraud resistance was also questioned many times over the years, in particular, because of the assumption that the prover does not want to reveal his secret key to his accomplice. If he trusts the accomplice enough to let him authenticate once, then why would he not trust him to delete the information he learnt after the protocol? Actually, a recent article [8] shows that terrorist-fraud resistance is in fact irrelevant, under the assumption that tamper-proof devices can be built. Two cases are identified by [8]. One, the prover does not know his secret key (black-box model) and therefore he cannot meaningfully help an accomplice. Or, the prover knows his secret key (white-box model) and so he can build a full tamper-proof, single-use copy of his device and give it to his accomplice; the accomplice authenticates once with this device, and does not learn any additional information as the device is tamper-proof and it is built to wipe its memory after one authentication.

Assumption 7: Use of Cryptographic Keys. The vast majority of existing distance-bounding protocols rely on cryptographic keys as a means of authentication.

Two DB protocols [25, 28] use physically uncloneable functions (PUFs) instead. The advantage is that, contrary to a cryptographic key, a PUF is designed to be untransferable. However, dishonest provers can bypass PUFs' untransferability (in the BadPUF model [33]). This limits the interest of using PUFs instead of keys in distance bounding, where dishonest provers are customary.

3 GOING FURTHER

We now move on from debatable assumptions to future endeavours.

Dishonest provers. Security properties related to dishonest provers do not seem to be a priority for real-life distance-bounding applications. In particular, the protocols by NXP and Mastercard are both vulnerable to distance fraud, distance hijacking and terrorist fraud: a dishonest, far away prover can send his response in advance, since the latter is independent of the challenge.

We believe these attacks should be considered seriously by the industry. For instance, imagine a military facility: the people inside have access to real-time, sensitive information through a mobile app. A verifier uses (authenticated) distance bounding, to give access to the app only to people who are inside the facility. Now assume a secret meeting occurs inside this facility. It should be impossible for someone not invited to the meeting to have access to the data exchanged via the app. However, if the DB protocol is vulnerable to distance fraud, or distance hijacking, a malicious user can access the app from outside the building. Similarly, assume the app grants different levels of privilege and information, depending on the rank of the user: if a malicious general is not invited to the meeting, he could perform a terrorist fraud with the help of a lower-ranked accomplice (e.g., a security guard), and allow this accomplice to have access to information that he is not allowed to see.

In the case of payment systems, distance fraud should also be counteracted, as it could be used by a criminal to obtain an alibi. They could use a distance fraud to pay for goods in a shop, while they are actually somewhere else committing a crime; the payment log from the shop's terminal would make them appear innocent. Distance-fraud counteraction in contactless payments is even more acutely called for by the fact that recent proposals [38] enforce proximity-checks be added to banks' payment-logs as well.

No Tamper-proof Devices and Terrorist Fraud. In the previous section, we mentioned that terrorist-fraud resistance could be ignored in distance bounding. However, this only holds if tamper-proof devices can be built (otherwise, the strategy for terrorist-fraud resistance described in [8] does not work). Without tamper-proof devices, we are back to needing terrorist-fraud resistance. This brings us to questioning an implicit assumption made in terrorist-fraud resistant protocols: the accomplice A follows the instructions of the prover P^*. However, if the A deviates from the instructions of P^*, he can sometimes obtain the possibility to authenticate later. For instance, consider the directional attacks proposed in [2], in which the terrorist fraud succeeds only because P^* can use a directional antenna to send the verifier a message that A cannot read. If A can read this message, then he could authenticate on his own later, and the terrorist fraud would therefore be unsuccessful. Hence, the attack can work only if A complies with staying in a position where the messages sent through the directional antenna cannot reach him. Yet, A does not have to be in the line-of-sight between P^* and the verifier: he could simply hide a receiver near the verifier, and read the directional message afterwards. From this, a new research direction possibly arises: *should a terrorist-fraud accomplice A be considered as executing an algorithm predefined by his helper P^*, or not?* Similarly, if P^* choses the algorithm run by A, can a third-party adversary obtain information during the attack?

Moreover, the recent formalism in [14] mentions a variation of terrorist fraud, in which the accomplice is a legitimate prover, holding a valid key. To what extent does this affect existing protocols?

Multiple Verifiers. Academic DB protocols consider that a prover authenticates to a single verifier at a time. On the one hand, when tackling distance fraud, it is natural to ask whether multiple verifiers could aid. That is, the prover could be placed in the middle of several verifiers, each of them performing the same measurements simultaneously and comparing the results. For such a countermeasure, a different threat model is required: it should consider provers with multiple devices at different locations. On the other, multiple verifiers performing time-measurements at the same time may not (easily) help against terrorist fraud. Yet, DB protocols with more than two parties were proposed in the literature: e.g., [13].

Non-Identifiable Devices and Provers. The very principle of relay attacks requires that the adversary can present a fraudulent device that looks like a legitimate prover to the verifier. Indeed, if the verifier, or optionally the person operating it, could distinguish a counterfeited prover device from a legitimate one, there would be no relay attack (in the standard sense of the word). An idea is to add a biometric identification of the card-holders onboard the cards and/or readers. Contactless bankcards with fingerprint readers onboard are being tried out [30], to prevent someone fraudulently use a contactless card lost by someone else. Note that this measure alone would not stop relaying altogether, instead it would restrict it to "online relaying": the attacker needs to commence the relaying (from one POS to another) after the fingerprint was read.

A more robust idea would be to add fingerprint-reading onboard RFID/NFC cards as well as RFID/NFC readers. Presuming robust biometry and the refusal to operate if the readings do not match stored biometrics, fingerprint-readings both from card and readers at once would eliminate the need for distance bounding altogether: the legitimate holder of the proving device would have to be physically present for the authentication to be accepted. However, such a solution is hard to deploy at a large scale (e.g., biometric data is generally not spread widely and is stored in HSMs which when queried answer just "yes/no"), ethically debatable and security/privacy sensitive. Small-scale solutions of this type (e.g., in a high-security small unit) could however be envisaged. Moreover, this approach would only work for protocols involving humans. Yet, humans only represent a small portion of the future uses of DB: i.e., with the advent of autonomous connected vehicles, there will be a great need for relay protection to prevent maliciously induced accidents.

Mobile (Mutual) Verifiers. In academic DB, verifiers do not move and the measurements are w.r.t. their fixed location. One challenge brought about by connected devices is that the verifiers in DB will constantly change their position. Moreover, both provers and verifiers would both be mobile and with an acute need for their authentication and time-measurements to be mutual, a la the aforementioned [6, 12]. To this end, image an autonomous platoon of smart, connected cars and constantly measuring the relative distance between themselves. The challenge of building mutually authenticated DB with mobile parties appears no mean feet.

Computational Power and Time Measurement. In academic DB, computation of timed responses is generally constrained to be as simple as possible, typically a table lookup or a bitwise XOR between the challenge and some precomputed response bit. The reason is as follows: if the computation time is large, and even if this time is predictable, a malicious prover can use more powerful hardware to respond faster. Additionally, depending on the physical layer, a mafia-fraud adversary could send messages to the prover at a higher frequency in order to make the prover respond faster. Since information is transmitted at the speed of light, an adversary gaining a few microseconds can cheat by several kilometres.

Yet, we believe that complex response functions should however be allowed.First, most distance-bounding protocols were designed for RFID tags, which do indeed have low computational power. However, today's relay-counteractions cannot be restricted to the RFID context. For instance, contactless payments via smartphones are nowadays common. Additionally, devices which can possibly embed a large and powerful distance-bounding apparatus also need relay protection: e.g., warplanes aim to counter the well-known MIG-in-the-middle [3] attack, in which an enemy plane impersonates an ally one through relaying. Moreover, lightweight cryptographic primitives are gaining interest int the context of the internet of things. In particular, low-latency ciphers, such as PRINCE [7], provide "instantaneous encryption", *i.e.*, encryption within a single clock cycle. Therefore, we argue that, within a few years, distance bounding using specialised hardware will be capable of running protocols using cryptographic primitives in the timed exchanges.

The `SimpleDB-Enc` Protocol. Lifting the aforementioned assumption that cryptography cannot be used during the timed phase, we propose a secure distance-bounding protocol called `SimpleDB-Enc`: the prover sends a nonce N_P, as well as his identity P, the verifier sends a n-bit challenge C, and the prover replies with $R = \mathbb{E}_x(N_P, C)$, where $\mathbb{E}$ is a symmetric cipher, and x is a shared key. This protocol provably resists all threats against distance bounding including terrorist fraud, in the ideal cipher model [34], assuming the computation of the response is instantaneous or short with regards to the time bound of the verifier.

4 CONCLUSIONS

We analytically discussed the validity of standard assumptions w.r.t. DB design-constraints and threat-models. Then, we elaborated on the future of DB. We also proposed a new simple and secure high-level design that lifts the important DB assumption of no cryptographic operations during the timed phase. We believe that such protocols are the future of DB, alongside other promising candidates such as quantum distance bounding [1].

REFERENCES

[1] Aysajan Abidin, Eduard Marin, Dave SingelÃľe, and Bart Preneel. 2016. Towards Quantum Distance Bounding Protocols. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 10155 (11 2016). DOI : https://doi.org/10.1007/978-3-319-62024-4_11

[2] Ahmad Ahmadi and Reihaneh Safavi-Naini. 2018. Directional Distance-Bounding Identification. In *Information Systems Security and Privacy*, Paolo Mori, Steven Furnell, and Olivier Camp (Eds.). Springer International Publishing, Cham, 197–221.

[3] Ross J. Anderson. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems* (2 ed.). Wiley Publishing.

[4] Gildas Avoine, Muhammed Ali Bingöl, I. Boureanu, Srdjan Čapkun, Gerhard Hancke, Süleyman Kardaş, Chong-Hee Kim, Cédric Lauradoux, Benjamin Martin, Jorge Munilla, Alberto Peinado, Kasper Bonne Rasmussen, Dave Singelée, Aslan Tchamkerten, Rolando Trujillo Rasua, and Serge Vaudenay. 2018. Security of Distance-Bounding: A Survey. *Comput. Surveys* (2018).

[5] G. Avoine, X. Bultel, S. Gambs, D. Gérault, P. Lafourcade, C. Onete, and J. Robert. 2017. A Terrorist-fraud Resistant and Extractor-free Anonymous Distance-bounding Protocol. In *Proc. of ASIA CCS ’17*. ACM, 800–814.

[6] G. Avoine and C. H. Kim. 2013. Mutual Distance Bounding Protocols. *IEEE Transactions on Mobile Computing* 12, 5 (May 2013), 830–839. DOI : https://doi.org/10.1109/TMC.2012.47

[7] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, and others. 2012. Prince–a low-latency block cipher for pervasive computing applications. In *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 208–225.

[8] Ioana Boureanu, David Gerault, and Pascal Lafourcade. 2018. Implementation-Level Corruptions in Distance Bounding – Exhibiting Faults and Provably-Secure Fixes in the Electronic Payment Protocol PayPass –. Cryptology ePrint Archive, Report 2018/1243. (2018). https://eprint.iacr.org/2018/1243.

[9] Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. 2015. Practical and Provably Secure Distance-Bounding. *Journal of Computer Security* 23, 2 (2015), 29. 229–257. DOI : https://doi.org/10.3233/Jcs-140518

[10] Stefan Brands and David Chaum. 1994. Distance-bounding Protocols. In *Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT ’93)*. Springer-Verlag, Berlin, Heidelberg, 344–359. http://dl.acm.org/citation.cfm?id=188307.188361

[11] Agnès Brelurut, David Gerault, and Pascal Lafourcade. 2016. Survey of Distance Bounding Protocols and Threats. In *Foundations and Practice of Security*, Joaquin Garcia-Alfaro, Evangelos Kranakis, and Guillaume Bonfante (Eds.). Springer International Publishing, Cham, 29–49.

[12] Srdjan Capkun, Levente Buttyan, and Jean-Pierre Hubaux. 2003. SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. *SASN* (2003), 12. http://infoscience.epfl.ch/record/489

[13] Srdjan Capkun, Karim El Defrawy, and Gene Tsudik. 2011. Group distance bounding protocols. In *International Conference on Trust and Trustworthy Computing*. Springer, 302–312.

[14] Tom Chothia, Joeri De Ruiter, and Ben Smyth. 2018. Modelling and Analysis of a Hierarchy of Distance Bounding Attacks. In *Proceedings of the 27th USENIX Conference on Security Symposium (SEC’18)*. USENIX Association, Berkeley, CA, USA, 1563–1580. http://dl.acm.org/citation.cfm?id=3277203.3277320

[15] Jolyon Clulow, Gerhard P Hancke, Markus G Kuhn, and Tyler Moore. 2006. So near and yet so far: Distance-bounding attacks in wireless networks. In *European Workshop on Security in Ad-hoc and Sensor Networks*. Springer, 83–97.

[16] B. Danev. 2018. METHOD , DEVICE AND SYSTEM FOR SECURE DISTANCE MEASUREMENT. (2018). US patent 20180367994.

[17] Alexandre Debant, Stéphanie Delaune, and Cyrille Wiedling. 2018. *Proving physical proximity using symbolic models*. Research Report. Univ Rennes, CNRS, IRISA, France. https://hal.archives-ouvertes.fr/hal-01708336

[18] D. Dolev and A. Yao. 1983. On the Security of Public-Key Protocols. *IEEE Transactionson Information Theory 29* 29, 2 (1983).

[19] Ulrich Dürholz, Marc Fischlin, Michael Kasper, and Cristina Onete. 2011. A Formal Approach to Distance-Bounding RFID Protocols. In *Information Security*, Xuejia Lai, Jianying Zhou, and Hui Li (Eds.). Lecture Notes in Computer Science, Vol. 7001. Springer Berlin Heidelberg, 47–62. DOI : https://doi.org/10.1007/978-3-642-24861-0_4

[20] EMVCo. 2018. Book C-2 Kernel 2 Specification v2.7. EMV Contactless Specifications for Payment System. www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/C-7_Kernel_7_V_2_7_Final.pdf. (Feb, 2018).

[21] Marc Fischlin and Cristina Onete. 2013. Terrorism in Distance Bounding: Modeling Terrorist Fraud Resistance. In *Proceedings of ACNS 2013 (LNCS)*, Vol. 7954. Springer Verlag, 414–431.

[22] G. Hancke. 2012. Distance-bounding for RFID: Effectiveness of ’terrorist fraud’ in the presence of bit errors. In *2012 IEEE International Conference on RFID-Technologies and Applications, RFID-TA 2012, Nice, France, November 5-7, 2012*. 91–96.

[23] I. Boureanu and Anda Anda. 2018. Another Look at Relay and Distance-based Attacks in Contactless Payments. Cryptology ePrint Archive, Report 2018/402. (2018). https://eprint.iacr.org/2018/402.

[24] I. Boureanu and Serge Vaudenay. 2014. Optimal Proximity Proofs. In *Information Security and Cryptology - 10th International Conference, Inscrypt 2014, Beijing, China, December 13-15, 2014, Revised Selected Papers*. 170–190.

[25] Mathilde Igier and Serge Vaudenay. 2016. Distance Bounding Based on PUF. In *Cryptology and Network Security*, Sara Foresti and Giuseppe Persiano (Eds.). Springer International Publishing, Cham, 701–710.

[26] Handan Kilinc. 2018. Implications of Position in Cryptography. (2018), 209. DOI : https://doi.org/10.5075/epfl-thesis-8981

[27] Handan Kılınç and Serge Vaudenay. 2015. Optimal Proximity Proofs Revisited. In *Applied Cryptography and Network Security*, Tal Malkin, Vladimir Kolesnikov, Allison Bishop Lewko, and Michalis Polychronakis (Eds.). Springer International Publishing, Cham, 478–494.

[28] S. Kleber, R. W. van der Heijden, H. Kopp, and F. Kargl. 2015. Terrorist fraud resistance of distance bounding protocols employing physical unclonable functions. In *2015 International Conference and Workshops on Networked Systems (NetSys)*. 1–8. DOI : https://doi.org/10.1109/NetSys.2015.7089068

[29] S. Mauw, Z. Smith, J. Toro-Pozo, and R. Trujillo-Rasua. 2018. Distance-Bounding Protocols: Verification without Time and Location. In *S&P 2018*. Springer. DOI : https://doi.org/10.1109/SP.2018.00001

[30] Stephen Mayhew. 2018. Korean credit card companies developing biometrics-based offline payments system. https://www.biometricupdate.com/201806/korean-credit-card-companies-developing-biometrics-based-offline-payments-system. (2018).

[31] Catherine Meadows, Radha Poovendran, Dusko Pavlovic, LiWu Chang, and Paul Syverson. 2007. Distance bounding protocols: Authentication logic analysis and collusion attacks. In *Secure localization and time synchronization for wireless sensor and ad hoc networks*. Springer, 279–298.

[32] Ricardo J Rodríguez. 2017. Evolution and characterization of point-of-sale RAM scraping malware. *Journal of Computer Virology and Hacking Techniques* 13, 3 (2017), 179–192.

[33] Ulrich Ruhrmair and Marten van Dijk. 2013. PUFs in Security Protocols: Attack Models and Security Evaluations. In *Proceedings of the 2013 IEEE Symposium on Security and Privacy (SP ’13)*. IEEE Computer Society, Washington, DC, USA, 286–300. DOI : https://doi.org/10.1109/SP.2013.27

[34] Claude E Shannon. Communication theory of secrecy systems. (????).

[35] Mridula Singh, Patrick Leu, and Srdjan Capkun. 2017. UWB with Pulse Reordering: Securing Ranging against Relay and Physical Layer Attacks. *IACR Cryptology ePrint Archive* 2017 (2017), 1240.

[36] T. Chothia, Flavio D. Garcia, Joeri de Ruiter, Jordi van den Breekel, and Matthew Thompson. 2015. Relay Cost Bounding for Contactless EMV Payments. In *Financial Cryptography and Data Security - 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers (Lecture Notes in Computer Science)*, Rainer Böhme and Tatsuaki Okamoto (Eds.), Vol. 8975. Springer, Puerto Rico, 189–206.

[37] Peter Thueringer, Hans De Jong, Bruce Murray, Heike Neumann, Paul Hubmer, and Susanne Stern. 2008. Decoupling of measuring the response time of a transponder and its authentication. (November 2008).

[38] Liqun Chen Tom Chothia, Ioana Boureanu. 2019, to appear. Making Contactless EMV Payments Robust Against Rogue Readers Colluding With Relay Attackers. In *the 23rd International Conference on Financial Cryptography and Data Security (Financial Crypto 2019)*.

[39] Serge Vaudenay. 2013. On Modeling Terrorist Frauds. In *Proceedings of the 7th International Conference on Provable Security - Volume 8209 (ProvSec 2013)*. Springer-Verlag, Berlin, Heidelberg, 1–20. DOI : https://doi.org/10.1007/978-3-642-41227-1_1