cryptography

MDPI

Article

On Detecting Relay Attacks on RFID Systems Using Qubits

Aysajan Abidin

imec-COSIC KU Leuven, Kasteelpark Arenberg 10-bus 2452, 3001 Heverlee, Belgium; aysajan@kuleuven.be

Received: 31 October 2019; Accepted: 5 May 2020; Published: 8 May 2020

Abstract: As RFID technology is being widely used in access control systems to identify and track both objects and people, relay attacks on RFID systems continue to pose serious threats to security. To mitigate relay attacks, distance bounding protocols can be used. Until recently, all distance bounding protocols were based on classical cryptography and communication techniques. In this paper, we take a closer look at a recently proposed protocol by Jannati and Ardeshir-Larijani [Quantum Information Processing 2016, 18] to detect relay attacks using qubits. We first observe that the protocol has a weakness which allows an adversary to mount a successful attack on the protocol. We then propose a countermeasure to restore security and compare the fixed protocol with the state of the art.

Keywords: relay attack; distance bounding; RFID systems; quantum communication; quantum cryptography

1. Introduction

Today wireless embedded systems are ubiquitous in almost all aspects of our daily lives. Their ever growing use is also making them increasingly complex. For instance, what used to be a reader or a passive tag in a single closed application, an RFID (radio-frequency identification) has become a core Internet-of-Things (IoT) technology with multiple uses in identification, alerting, monitoring, and authentication; no longer a simple reader or tag. As a result, RFID technology is integrated into wireless systems such as contactless payment systems, access control, e-ID/e-passport, supply chain management, etc. Although the communication range of the devices used in such systems is limited, they are vulnerable to relay attacks, as demonstrated in [1]. In a relay attack, an adversary attempts to fool the legitimate parties by simply relaying the communication between them. Without doubt, relay attacks pose serious security risks to wireless systems.

As a countermeasure against relay attacks, a distance bounding (DB) protocol is introduced by Brands and Chaum in [2]. A DB protocol allows to establish an upper-bound on the physical distance between two communicating parties, commonly called as a verifier and a prover. Since its introduction by Brands and Chaum, many DB protocols are designed and implemented [3–17]. A DB protocol typically comprises an initialisation phase and a fast bit-exchange phase. The fact that it is impossible for adversaries to send bits faster than the legitimate parties, which is the case in RF-based DB protocols, is used to estimate an upper bound on the physical distance between them. DB protocols provide an effective countermeasure against relay attacks. However, secure implementation of the fast-bit exchange phase for distance bounding has been a challenge.

In [18], Jannati and Ardeshir-Larijani propose to use qubits for detecting relay attacks on RFID systems. In particular, they propose a RAD (relay attack detection) protocol which basically replaces the fast-bit exchange phase of a DB protocol with a phase in which the prover sends qubits to the verifier. In this paper, we take a closer look at the RAD protocol and observe its weaknesses. We show that the RAD protocol does not offer protection against relay attacks, since an adversary equipped

with quantum memory can easily mount relay attacks. We further discuss possible countermeasures to mitigate the weaknesses of the RAD protocol.

The rest of the paper is organized as follows. Section 2 provides the necessary background material facilitating the understanding of the paper. Section 3 presents the RAD protocol by Jannati and Ardeshir-Larijani, and its vulnerability against relay attacks. In Section 4, we propose a countermeasure, analyse its security, and compare it with state of the art. After presenting related work in Section 5, we conclude the paper in Section 6.

2. Background

In this section we present some background material. We begin by recalling the distance bounding protocol by Hancke and Kuhn [3], since it is most relevant to the RAD protocol. Following [18], we also call the verifier and the prover, the reader and the tag, respectively, from now on.

2.1. Distance Bounding

In general, a DB protocol consists of an initialisation and a rapid-bit exchange (a.k.a. *distance-bounding*) phase. In the initialisation phase, the reader and the tag exchange some public information, namely, public nonces, that will allow them to compute a common value using a preshared key. In the rapid-bit exchange phase, the reader sends a sequence of single-bit challenges to which the tag replies with single-bit responses. The distance of the tag to the reader is calculated by measuring the Round-Trip Time (RTT) of the challenge-response bits between the reader and the tag. If a DB protocol is derived from the original Brands-Chaum protocol [2], then a last *authentication phase* is also needed for checking whether all protocol steps are followed correctly. But the Hancke-Kuhn protocol [3] that we are going to look at next comprises only the initialisation and the distance-bounding phases.

Figure 1 illustrates the Hancke-Kuhn [3] protocol. The reader and the tag have a shared secret key K. In the *initialisation phase* the reader and the tag exchange with each other the randomly generated nonces N_T and N_R. They then calculate the response registers $D||B = PRF_K(N_R, N_T)$, where PRF is a pseudorandom function and $||$ stands for concatenation. The *rapid-bit exchange phase* consists of many rounds of time-critical single bit challenge-responses. The number of challenge-response rounds is depends on the targeted security level and is equal to the length of the registers $|D|$ or $|B|$. In a challenge-response round i, the reader starts its clock and sends to the tag randomly chosen challenge bit $C_i \in \{0, 1\}$, to which the tag responds either with $R_i = D_i$ if $C_i = 0$, or with $R_i = B_i$ otherwise. The reader stops the clock as soon as it receives the response R_i. Then the reader compares the received responses with the expected responses. If the responses are correct, it checks whether the round-trip time $\Delta t_i < \tau_{RTT}$, where τ_{RTT} is the maximum round-trip time for a bit to travel between the reader and the tag. If all checks pass, then the tag is identified as close by and is authenticated. Note that the protocol can be made to tolerate errors by setting a threshold for the number of correct responses.

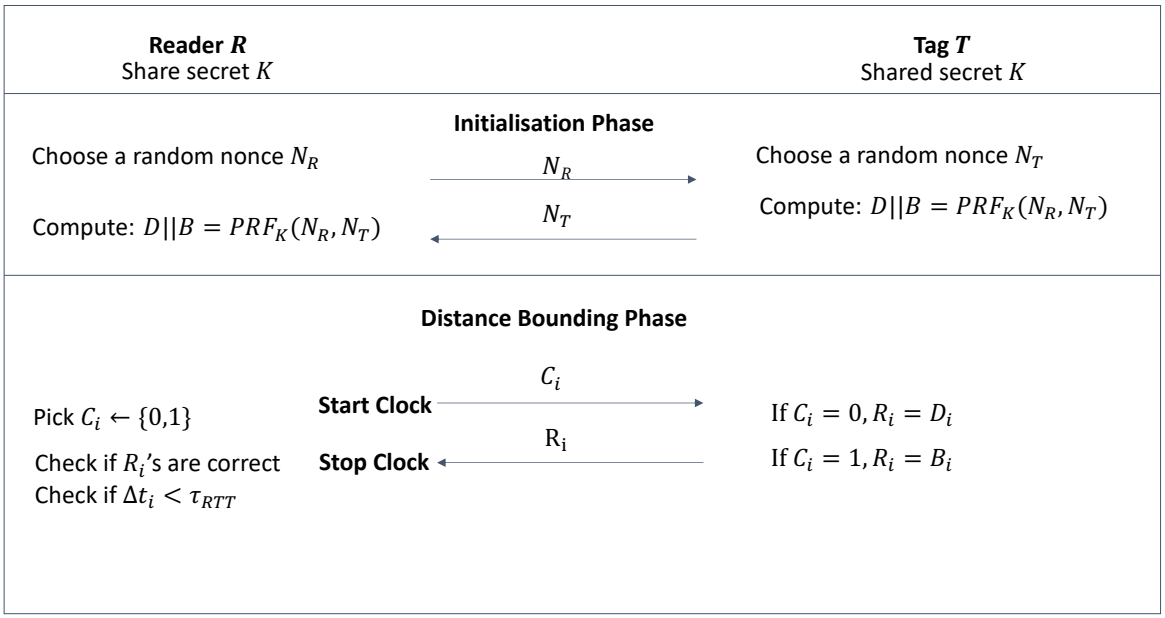

Figure 1. A distance bounding protocol by Hancke and Kuhn [3].

2.2. Qubits

A qubit is a basic element of quantum information, just as a bit is the basic element of classical information. A qubit is a vector in a 2-dimensional Hilbert space, a vector space with inner product. The basis

$$\{|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}\}$$

for a qubit is called the computational basis, whereas the basis

$$\{|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, \ |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\}$$

is called the Hadamard basis. In general, we can express a normalised quantum state as a superposition of $|0\rangle$ and $|1\rangle$ as

$$\alpha\,|0\rangle + \beta\,|1\rangle\,,$$

where $\alpha, \beta \in \mathbb{C}$ satisfying $|\alpha|^2 + |\beta|^2 = 1$.

If we measure a qubit in state $\alpha\,|0\rangle + \beta\,|1\rangle$ in the computational basis, then we obtain $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$. Upon measurement, the state $\alpha\,|0\rangle + \beta\,|1\rangle$ of the qubit collapses into $|0\rangle$ or $|1\rangle$, depending on the measurement outcome.

The four states, $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$, satisfy that

$$|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$$

and

$$|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}.$$

If we measure the qubits $|0\rangle$ and $|1\rangle$ in the computational basis, then the states do not change; whereas a measurement in the Hadamard basis destroys the state completely. In the latter case, we obtain either $|+\rangle$ or $|-\rangle$ with equal probability. Similarly, if we measure the qubits $|+\rangle$ and $|-\rangle$ in the Hadamard basis, then the states do not change; whereas a measurement in the computational basis destroys the state, and we obtain either $|0\rangle$ or $|1\rangle$ with equal probability. This is the basic principle behind many quantum cryptographic protocols, most notably, the Quantum Key Distribution (QKD) protocol by Bennet and Brassard [19]. The authors of [18] also use this principle to replace

the distance-bounding phases of a DB protocol with a *qubit transmission phase*, as we shall see in the next section.

We can associate these four states with different polarisations of photons: The states $|0\rangle$ and $|1\rangle$ with horizontally $\rightarrow$ and vertically $\uparrow$ polarised photons, respectively, and the states $|+\rangle$ and $|-\rangle$ with $\nearrow$ (45°) and $\nwarrow$ (-45°) polarised photons, respectively. We can encode classical information into these four state. For example, we can encode the classical bit value 0 as a qubit in state $|0\rangle$ or $|+\rangle$, and the value 1 as a qubit in state $|1\rangle$ or $|-\rangle$. We measure the qubits either in the computational or the Hadamard basis to extract the encoded information. Let us denote by 0 the computational $(+)$ basis and by 1 the Hadamard $(\times)$ basis. Then a classical to quantum encoding rule may look like as in Table 1. If we encode 0 as $\rightarrow$ polarized photon, then we can decode it correctly as 0 only in the $+$ basis, whereas if we encode 0 as $\nearrow$ polarized photon, then we can decode correctly as 0 only in the $\times$ basis. This also applies to the case when we encode 1 in the $+$ basis and the $\times$ basis, respectively. In any of these cases, if we decode a polarized photon using a wrong basis, then we obtain a completely random bit. Therefore, by using this encoding rule we can send information encoded as polarized photons so that no one can copy or read the information without knowing the bases we use for encoding.

Table 1. A classical to quantum encoding rule.

Data	Comp. (or $+$) Basis	Hadamard (or $\times$) Basis
0	$\|0\rangle$ (i.e., $\rightarrow$)	$\|+\rangle$ (i.e., $\nearrow$)
1	$\|1\rangle$ (i.e., $\uparrow$)	$\|-\rangle$ (i.e., $\nwarrow$)

3. Rad Protocol and Its Weaknesses

In this section we first take a closer look at the protocol for relay attack detection, namely, the RAD protocol, using qubits proposed in [18]. We then observe its weaknesses and show that it is still vulnerable to relay attacks.

3.1. The Protocol

In a DB protocol, the distance-bounding phase is the time critical and the most difficult phase to implement in practice. The authors of [18] mention the challenges in accurate RTT measurement as one of the main motivating reasons for the RAD protocol, since it does not require any RTT measurements in the qubit transmission phase.

Figure 2 presents the RAD protocol from [18]. As shown in the figure, the protocol comprises two phases: an initialisation phase and a qubit transmission phase. The initialisation phase is the same as in the Hancke-Kuhn DB protocol presented in Figure 1. The qubit transmission phase replaces the distance-bounding phase of a DB protocol. In this phase, upon receiving a request from the reader, the tag prepares quantum states $|D\rangle$ according to bases determined by B, and sends $|D\rangle$ to the reader. The reader then measures the received photons in his copy of B, and checks whether the measurement results, say, D', equal D. If $D = D'$, then the tag is accepted as valid; otherwise, it is regarded as relay attack detection.

As an application of the RAD protocol, the authors of [18] applied it to improve an ultra-lightweight RFID authentication protocol by Gao et al. [20].

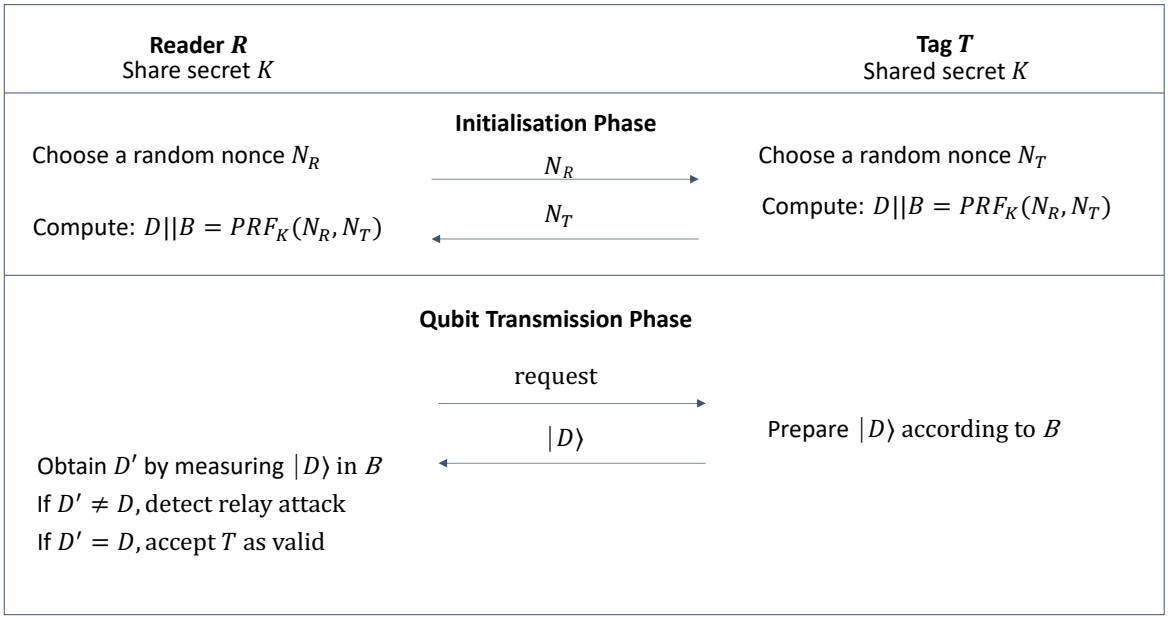

Figure 2. RAD protocol using qubits for relay attack detection [18].

3.2. Weaknesses

In [18], the authors analysed the security of the RAD protocol against an intercept-resend type of relay attack. In particular, a relay attack adversary first intercepts the photons from the tag, measures them in random bases since it does not know the right bases, and then sends the measured results encoded as qubits to the reader. Figure 3 illustrates the attack considered by the authors of [18]. Indeed, in this attack, the adversary can successfully relay a qubit with probability $3/4$, since the adversary has to guess the measurement basis at random and use that basis to encode the measured result into new qubit. Note that in relay attacks on DB protocols, including the RAD protocol, the adversary simply relays everything in the initialisation phase. Hence, the initialisation phase in the attack figures is exactly the same as in the original protocol without any attack.

However, there is a better attack that the adversary can employ without being detected, as shown in Figure 4. In this attack, the adversary is equipped with a quantum memory capable of storing qubits. As said before, the adversary relays everything in the initialisation phase between the reader and the tag. In the qubit transmission phase, the adversary first pre-asks (i.e., before the reader sends its request) the tag to send its qubits and stores the qubits sent by the tag in the quantum memory. When the reader sends its request, the adversary replies with the qubits stored in the quantum memory. Since qubits stored in the quantum memory are the ones sent by the tag, the reader obtains the expected results upon measuring the qubits. Therefore, the attack goes unnoticed.

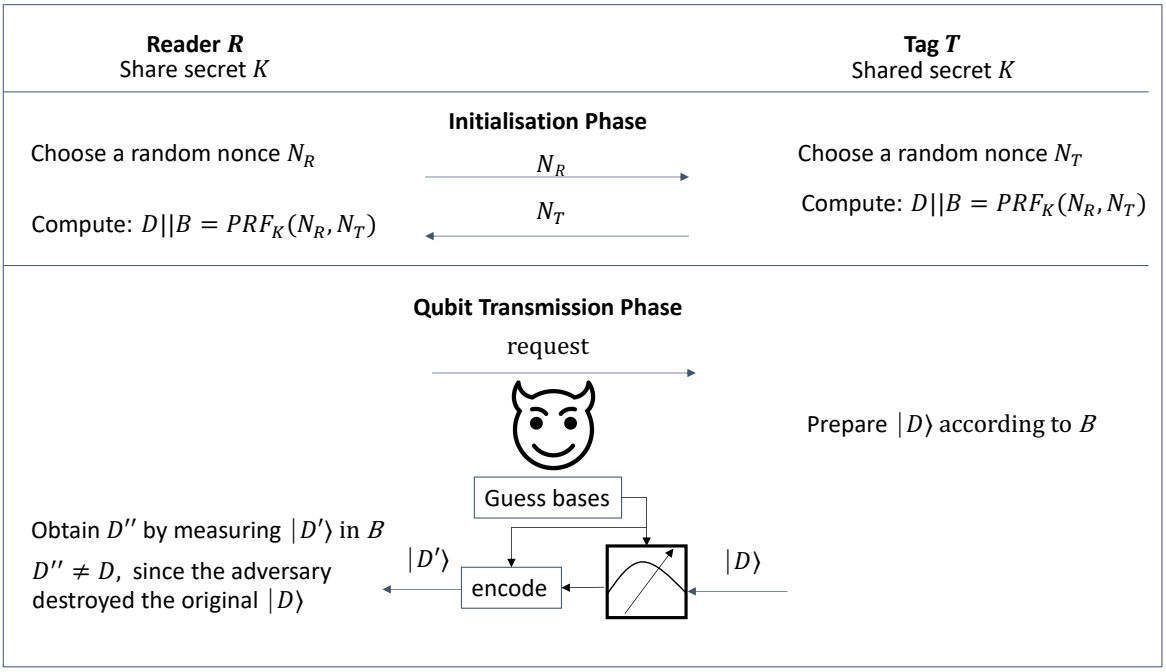

Figure 3. An intercept-resend relay attack on the RAD protocol.

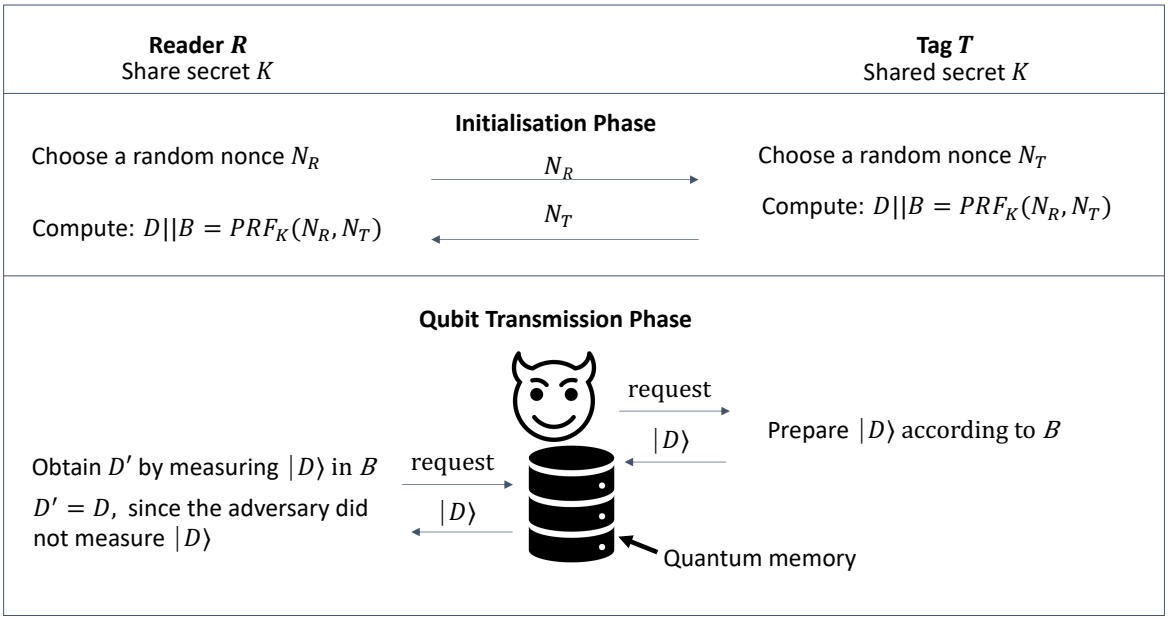

Figure 4. A relay attack on the RAD protocol by an adversary with quantum memory.

4. Countermeasure

The reason why the RAD protocol cannot effectively detect relay attacks, specially the one described in Figure 4, is because the protocol replaces the key component of a DB protocol that effectively mitigates relay attacks. Namely, the time-critical distance-bounding phase of a DB protocol is replaced with a qubit transmission phase that is *not* time-critical. DB protocols use round-trip time (RTT) of single bit challenge-responses in the time-critical phase between the prover and the verifier to calculate an upper bound on the distance between them. In the RAD protocol, however, there is no timing in the qubit transmission phase, which unfortunately makes the protocol vulnerable to relay attacks.

Yet another reason is that there is no dependence between the reader's "request" and the tag's response, as opposed to DB protocols. It is important to note, however, that a dependence of the tag's response on the reader's request, as in DB protocols, alone does not offer protection against relay attacks without any timing information.

Therefore, a fix to the RAD protocol to make it effective in relay attack detection is to introduce timing in the qubit transmission phase and a logical dependence of the tag's response on the reader's request. Figure 5 presents a modified RAD protocol. In this modified version of the RAD protocol, the qubit transmission phase is similar to the DB protocol presented in Figure 1. But now, the reader's challenge C_i, say, in round i of the qubit transmission phase, is encoded as $|C_i\rangle$ either using D_i as basis if $C_i = 0$, or using B_i as basis if $C_i = 1$. The reader measures the received qubit using D_i as basis if it sent 0 as challenge, otherwise it measures the qubit using B_i as basis. So the reader expects to obtain the same challenge bit when measuring the received qubits. In addition, each challenge-response round is timed, so the reader also checks whether the RTT is less than the RTT threshold.

This seemingly simple yet effective countermeasure turns the original RAD protocol into a DB protocol. This new protocol, which we call improved RAD protocol from now on, uses classical bits for challenges and qubits for responses. Below, we (a) analyse the security of the improved RAD protocol against common attacks on DB protocols, (b) compare it with the state of the art, and (c) provide a feasibility analysis.

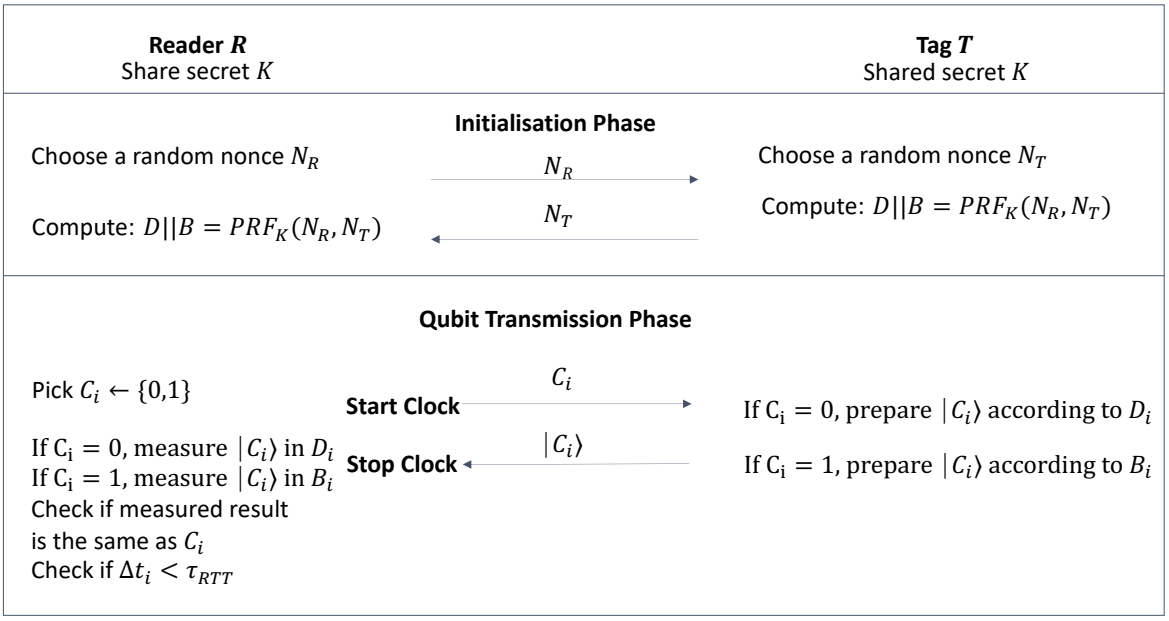

Figure 5. Improved RAD protocol.

4.1. Security of the Countermeasure

Here we analyse the security of the improved RAD protocol against distance fraud, mafia fraud (or relay attack), terrorist fraud, and distance hijacking. We assume that the bit length of D and B are n, respectively, and that qubit transmission phases comprises n rounds of challenge-response.

Distance fraud (DF). In this attack, a dishonest prover (or tag) attempts to shorten the distance to the verifier (or reader) by sending the responses before receiving the challenges by guessing them. Since the verifier chooses its challenges at random, the dishonest prover can only predict the challenge correctly with probability $1/2$ in each round. So, after n rounds of qubit transmission phase, the success probability will be $(1/2)^n$. The dishonest prover can also send a qubit encoding a random bit using either one of the two register values (B_i or D_i) as encoding basis as response. But the verifier will obtain the expected result with probability $1/2$. Therefore, distance fraud on the improved RAD protocol has a success probability of $(1/2)^n$.

Mafia fraud (MF) (or relay attack). This is a man-in-the-middle attack, whereby an adversary uses a proxy-prover close to the verifier and a proxy-verifier close to the honest prover to relay the messages exchanged between the prover and verifier over possibly a long distance [21]. In this attack, first the adversary simply relays the initialisation phase between the verifier and the prover, then executes qubit transmission phase with the prover, before the verifier starts it. Afterwards, it performs the qubit transmission phase with the verifier. In particular, the adversary asks the prover for responses for randomly chosen challenges in advance, then uses these responses to answer the verifier's actual challenges. So, there are two cases to consider in this attack:

- Case 1: the adversary's challenges match the verifier's challenges. In this case, the attacker can simply use the prover's responses, so the adversary succeeds with certainty.
- Case 2: the adversary's challenges do not match the verifier's challenges. In this case, the adversary knows which value to encode as a qubit to respond to the verifier, but there are two possible states to choose, since it does not know the register values which determine the basis, and in the state. So in this case the attacker succeeds with probability $1/2$.

Since *Case 1* and *Case 2* occur with equal probability $1/2$, attacker's total success probability is $3/4$ in one round of qubit transmission phase, or $(3/4)^n$ in n rounds.

Terrorist fraud. In this attack, a dishonest prover helps an adversary to prove to the verifier that it is in close proximity of the verifier, without leaking any information about its secret key. Terrorist-fraud resistant protocols are designed in such a way that revealing the values of B and D would reveal secret key K. Therefore, our improved RAD protocol is not terrorist fraud resistant in the current form. However, the scheme can be made resistant to terrorist frauds by letting $D = PRF_K(N_R, N_T)$, $B = \mathsf{Enc}_D(K)$, so that knowledge of D and B reveals K.

Distance hijacking. In this attack, a dishonest far away prover exploits honest provers that are located close to the verifier by hijacking their normal DB protocol execution [22]. Protocols that are derived from the original Brands and Chaum protocol [2] are vulnerable to distance hijacking, as they allow the attacker to highjack the messages sent from the prover to the verifier in the last phase of the protocol. Hancke and Kuhn protocol and others that are derived from it are resistant against distance hijacking, specially in single-protocol environments [22], since these protocols use the shared key between the prover and the verifier. Our improved RAD protocol also protects against distance hijacking, since it uses the shared secret.

4.2. Comparison with the State of the Art

The improved RAD protocol is a hybrid DB protocol, in the sense that the challenge-response phase comprises both classical bits (for challenges) and qubits (for responses). In Table 2, we compare our protocol with two recently proposed quantum DB protocols (cf. Section 5) and two classical DB protocols from which all other DB protocols are derived. We refer to [23], and the references therein, for a recent survey on DB protocols. As we can see from the table, our protocol compares favourably with the state of the art.

Table 2. Comparison of the improved RAD protocol with classical and quantum DB protocols.

	Distance Fraud	**Mafia Fraud**
Brands-Chaum [2]	$\left(\frac{1}{2}\right)^n$	$\left(\frac{1}{2}\right)^n$
Hanke-Kuhn [3]	$\left(\frac{3}{4}\right)^n$	$\left(\frac{3}{4}\right)^n$
Quantum DB [16]	$\left(\frac{3}{4}\right)^n$	$\left(\frac{3}{4}\right)^n$
Quantum DB [17]	$\left(\frac{1}{2}\right)^{\mathsf{HD}(B,D)}$	$\max\left(\left(\frac{1}{2}\right)^{\mathsf{HD}(B,D)}, \left(\frac{5}{8}\right)^n\right)$
Improved RAD	$\left(\frac{1}{2}\right)^n$	$\left(\frac{3}{4}\right)^n$

4.3. Feasibility

In addition to classical hardware components needed for implementation of DB protocols, our protocol further requires quantum components for qubit preparation (on the prover side) and measurement (on the verifier side). Since these quantum components are part of currently available Quantum Key Distribution (QKD) technology, our protocol is readily feasible. In particular, the same experimental setup for the quantum transmission and measurement phase in QKD can be applied to implement our protocol. QKD has not only been experimentally tested [24], but also commercially available.

5. Related Work

Since this work is on relay attack detection using qubits, we only present DB protocols that use qubits. To the best of the author's knowledge, there are two recently proposed DB protocols [16,17] that employ qubits instead of classical bits for the challenge-response.

Figures 6 and 7 illustrates the protocols in [16,17], respectively. As can be seen from the figures, the protocol in [16] comprises also of a third phase in which the tag sends a Message Authentication Code (MAC) tag of a message composed of the measured challenges, nonces exchanged in the initialisation phase, and both the reader and the tag's IDs. The protocol in [17] improves upon the protocol in [16] to eliminate the need for the last authentication phase. Both of these protocols appear similar to the improved RAD protocol.

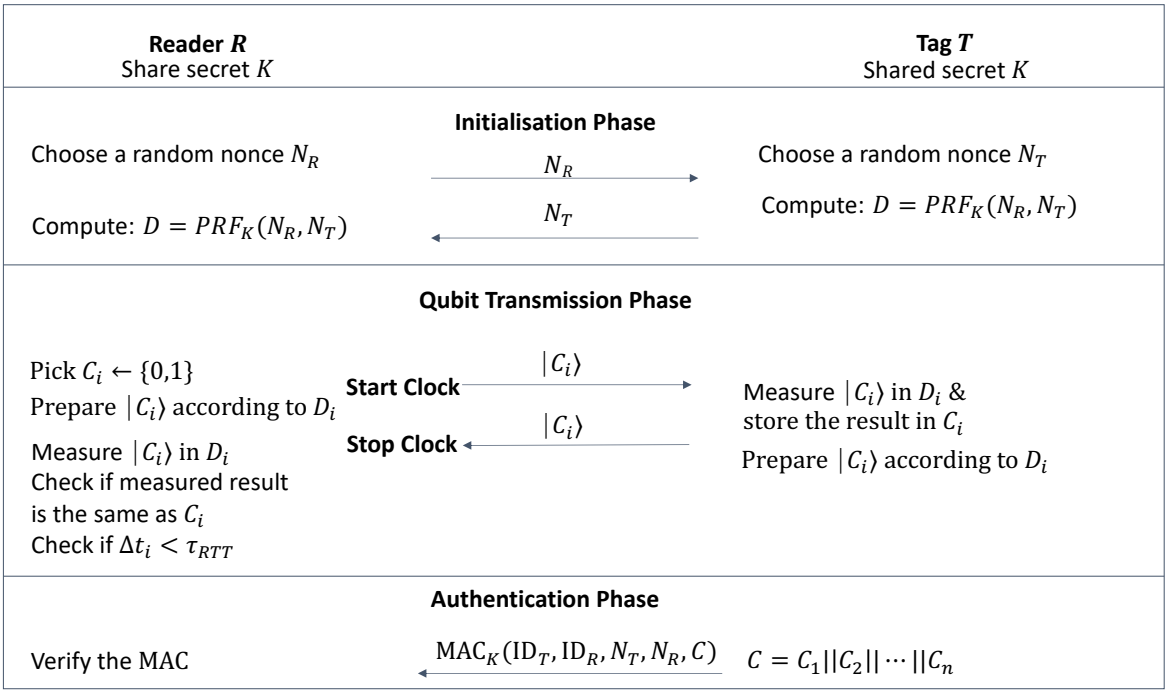

Figure 6. A quantum DB protocol proposed in [16].

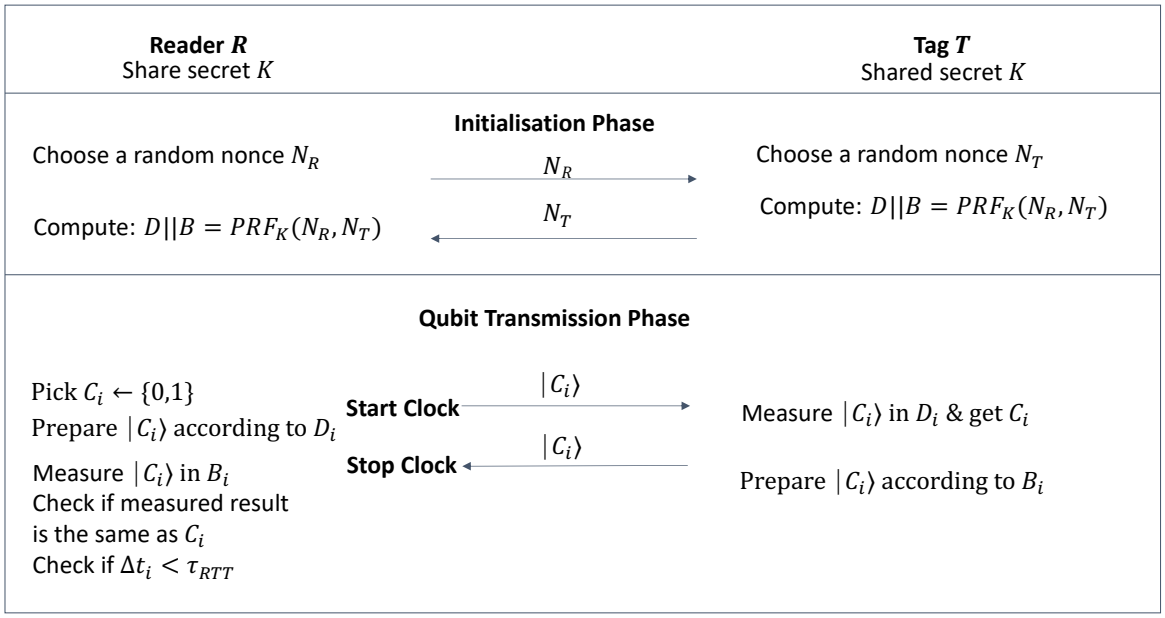

Figure 7. A quantum DB protocol proposed in [17].

6. Conclusions

Relay attacks pose serious security risks to RFID systems. Relay attacks can be mitigated by using distance bounding (DB) protocols, which involves accurate round-trip time (RTT) measurement. Since accurate RTT measurement introduces challenges in the implementation of DB protocols, a new RFID protocol, known as RAD protocol, for detecting relay attacks using qubits was proposed by Jannati and Ardeshir-Larijani [18]. In this paper we first showed that the RAD protocol is still vulnerable to relay attacks. We then improved upon the RAD protocol by basically turning the protocol into a DB protocol, and analysed its security. Finally, we compared our protocol with the state of the art, and briefly discussed its feasibility.

Funding: This work was supported by CyberSecurity Research Flanders with reference number VR20192203, by the Research Council KU Leuven: C16/15/058, and by imec through the Security & Privacy Centre projects on Secure Distance Bounding.

Conflicts of Interest: The author declares no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

DB	Distance bounding
RFID	Radio-Frequency Identification
IoT	Internet of Things
RAD	Relay attack detection
QKD	Quantum key distribution
PRF	Pseudo-random function
RTT	Round-trip time
MAC	Message Authentication Code

References

1. Francillon, A.; Danev, B.; Capkun, S. Relay attacks on passive keyless entry and start systems in modern cars. In Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 6–9 February 2011.

2. Brands, S.; Chaum, D. Distance-Bounding Protocols (Extended Abstract). In Proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, 23–27 May 1993.
3. Hancke, G.P.; Kuhn, M.G. An RFID Distance Bounding Protocol. In Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, SECURECOMM '05, Athens, Greece, 5–9 September 2005; IEEE Computer Society: Washington, DC, USA, 2005; pp. 67–73.
4. Clulow, J.; Hancke, G.; Kuhn, M.; Moore, T. So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks. In Proceedings of the 3rd European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS '06), Hamburg, Germany, 20–21 September 2006; pp. 83–97.
5. Tippenhauer, N.O.; Čapkun, S. ID-based Secure Distance Bounding and Localization. In Proceedings of the 14th European Conference on Research in Computer Security, Saint-Malo, France, 21–23 September 2009; Springer: Berlin/Heidelberg, Germany, 2009; pp. 621–636.
6. Rasmussen, K.B.; Čapkun, S. Realization of RF Distance Bounding. In Proceedings of the 19th USENIX Conference on Security, USENIX Security'10; USENIX, Washington, DC, USA, 11–13 August 2010; Association: Berkeley, CA, USA, 2010; p. 25.
7. Singelee, D.; Preneel, B. Distance Bounding in Noisy Environments. In Proceedings of the European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks (ESAS), Cambridge, UK, 2–3 July 2007; pp. 101–115.
8. Hancke, G.P. Design of a secure distance-bounding channel for RFID. *J. Netw. Comput. Appl.* **2011**, *34*, 877–887. [CrossRef]
9. Lee, S.; Kim, J.S.; Hong, S.J.; Kim, J. Distance bounding with delayed responses. *IEEE Commun. Lett.* **2012**, *16*, 1478–1481. [CrossRef]
10. Ranganathan, A.; Tippenhauer, N.O.; Škorić, B.; Singelée, D.; Čapkun, S. Design and Implementation of a Terrorist Fraud Resilient Distance Bounding System. In Proceedings of the Computer Security—ESORICS 2012: 17th European Symposium on Research in Computer Security, Pisa, Italy, 10–12 September 2012; Foresti, S., Yung, M., Martinelli, F., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 415–432.
11. Rasmussen, K.B.; Castelluccia, C.; Heydt-Benjamin, T.S.; Capkun, S. Proximity-based Access Control for Implantable Medical Devices. In Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS '09, Chicago IL, USA, 9–13 Novemner 2009; pp. 410–419.
12. Trujillo-Rasua, R.; Martin, B.; Avoine, G. Distance bounding facing both mafia and distance frauds. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 5690–5698. [CrossRef]
13. Ranganathan, A.; Danev, B.; Capkun, S. Proximity Verification for Contactless Access Control and Authentication Systems. In Proceedings of the 31st Annual Computer Security Applications Conference, ACSAC 2015, Los Angeles, CA, USA, 5–9 December 2015; ACM: New York, NY, USA, 2015; pp. 271–280. [CrossRef]
14. Tippenhauer, N.O.; Luecken, H.; Kuhn, M.; Capkun, S. UWB rapid-bit-exchange system for distance bounding. In Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, New York, NY, USA, 22 June 2015; p. 2.
15. Singh, M.; Leu, P.; Capkun, S. UWB with Pulse Reordering: Securing Ranging against Relay and Physical Layer Attacks; In Proceedings of the 26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, CA, USA, 24–27 February, 2019. [CrossRef]
16. Abidin, A.; Marin, E.; Singelée, D.; Preneel, B. Towards quantum distance bounding protocols. In *Radio Frequency Identification and IoT Security*; Springer: Berlin/Heidelberg, Germany, 2016; Volume 10155, pp. 151–162.
17. Abidin, A. Quantum Distance Bounding. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '19, Miami Beach, FL, USA, 14–17 May 2019; ACM: New York, NY, USA, 2019; pp. 233–238. [CrossRef]
18. Jannati, H.; Ardeshir-Larijani, E. Detecting relay attacks on RFID communication systems using quantum bits. *Quantum Inf. Process.* **2016**, *15*, 4759–4771. [CrossRef]
19. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 9–12 December 1984; IEEE: Bangalore, India, 1984; pp. 175–179.
20. Gao, L.; Ma, M.; Shu, Y.; Wei, Y. An ultralightweight RFID authentication protocol with CRC and permutation. *J. Netw. Comput. Appl.* **2014**, *41*, 37–46. [CrossRef]

21. Desmedt, Y. Major security problems with the "Unforgble" (Feige)-Fiat-Shamir proofs of identity and how to overcome them. In Proceedings of the SecuriCom, France, Paris, 15–17 March 1988; pp. 15–17.
22. Cremers, C.; Rasmussen, K.; Schmidt, B.; Capkun, S. Distance Hijacking Attacks on Distance Bounding Protocols. In Proceedings of the 2012 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 24–25 May 2012; pp. 113–127. [CrossRef]
23. Avoine, G.; Bingöl, M.A.; Boureanu, I.; Hancke, G.; Kardaş, S.; Kim, C.H.; Lauradoux, C.; Martin, B.; Munilla, J.; Peinado, A.; et al. Security of distance-bounding: A survey. *ACM Comput. Surv. (CSUR)* **2019**, *51*, 94. [CrossRef]
24. Gehring, T.; Händchen, V.; Duhme, J.; Furrer, F.; Franz, T.; Pacher, C.; Werner, R.F.; Schnabel, R. Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks. *Nat. Commun.* **2015**, *6*, 8795. [CrossRef] [PubMed]