

E-Passport: The Global Traceability or How to Feel Like an UPS Package

Dario Carluccio, Kerstin Lemke-Rust, Christof Paar, and Ahmad-Reza Sadeghi

Horst Görtz Institute for IT Security
Ruhr University Bochum
44780 Bochum, Germany
{carluccio,lemke,cpaar,sadeghi}@crypto.rub.de

Abstract. Since the introduction of RFID technology there have been public debates on security and privacy concerns. In this context the Machine Readable Travel Document (MRTD), also known as e-passport, is of particular public interest. Whereas strong cryptographic mechanisms for authenticity are specified for MRTDs, the mechanisms for access control and confidentiality are still weak.

In this paper we revisit the privacy concerns caused by the Basic Access Control mechanism of MRTDs and consider German e-passports as a use case. We present a distributed hardware architecture that can continuously read and record RF based communication at public places with high e-passport density like airports and is capable of performing cryptanalysis nearly in real-time. For cryptanalysis, we propose a variant of the cost-efficient hardware architecture (COPACOBANA) which has been recently realized.

Once, MRTD holder identification data are revealed, this information can be inserted into distributed databases enabling global supervision activities. Assuming RF readers and eavesdropping devices are installed in several different airports or used in other similar places, e.g., in trains, one is able to trace any individual similar to tracing packages sent using postal services such as UPS.

Keywords: E-Passport, Privacy, MRTD, Basic Access Control, RF Eavesdropper, MRTD Cracker, Biometrics.

1 Introduction

Radio-Frequency Identification (RFID) technology is already in wide deployment and has been incorporated into various applications [22]. RFID technology makes also tracing of individuals much easier, as human identification can entirely be performed automatically, even in an unnoticeable way. If compared to video surveillance, RFID technology further saves human post-processing of streaming data. Public debates on security and privacy issues have been raised since the introduction of RFID technology where one may get the impression that people are not concerned about privacy as long as the threat does not become tangible.

In this context the Machine Readable Travel Document (MRTD) also known as e-passport is of particular public interest. Currently, we are on the cusp of an RFID-based biometric technology which will have an impact on civil and personal rights for all of us.

The initiative for e-passports was started by organizations¹ in United States and several other countries to deploy biometric and RFID technologies for border and visa control. The claimed goal is to enhance security, protect against forgery and manipulation of travel documents and ease identity checks. On the one hand advocates of e-passports envisaged horrifying scenarios about terrorist attacks and other criminal activities. On the other hand advocates of data protection and civil rights have concerns regarding privacy and security. Hence, the initiative has been subject to many political and technical criticism. Several researchers have pointed out the security and privacy weaknesses of the deployed schemes and proposed improvements (see e.g., very well-written papers [11] and [12]). However, issuing states allowed for a very fast roll-out of e-passports. This was done although, compared to the traditional approach, the complexity of the system will be strongly increased: New cryptographic schemes must be deployed and new parties (e.g., chip and reader manufacturers, companies doing personalization of passports, service providers, Certification Authorities) are now involved making the underlying trust model, trust assumptions and trust relationships much more complex. An appropriate overall security evaluation of the realizations – especially concerning privacy aspects – seems to be either postponed or is made more difficult because of lack of public information. This is crucial since one expects that all basic principles of data protection law have to be observed when designing, implementing and using RFID technology.² These aspects are of great importance not only because the costs for issuing e-passports are imposed on citizens, e.g., by increasing the passport issuing fee³ but more importantly because they concern the security and privacy of citizens.

The cryptographic components of the e-passport scheme shall consist of a Passive Authentication, Basic Access Control (BAC), and an Active Authentication. Whereas Passive Authentication means that the data stored in an e-passport includes digital signatures by the issuing nation, Basic Access Control should setup a secured channel between the reader device (part of the inspection system) and the e-passport that assures both confidentiality and integrity of the data communication. Active Authentication is deployed for anti-cloning purposes requiring a digital signature scheme implemented on the e-passport chip. Note that both Basic Access Control and Active Authentication are optional mechanisms. Basic Access Control is already implemented, e.g., in Germany and the Netherlands. Current realizations of Basic Access Control deploy symmetric cryptography and generate the corresponding encryption and authentication keys from passport information that is visible in the physical passport document.

¹ More concretely, the International Civil Aviation Organization (ICAO)

² see, e.g., resolution on Radio Frequency Identification www.privacyconference2003.org/

³ e.g., from 26 to 59 EUR in Germany.

The scheme has been already successfully attacked using offline dictionary attacks⁴.

In this paper we revisit the privacy concerns of e-passports and show that more sophisticated devices, as we propose in this paper, can be built to defeat the user privacy when deploying the current realizations of e-passports (e.g., in Germany and the Netherlands). Further, we aim at providing a review of the measures taken and to point out the shortcomings in the entire process.

We propose a hardware architecture that can easily mount this kind of attacks in much shorter time, and even nearly real-time, i.e., the time needed to pass the inspection system. The implementation consists of two devices: The first one is a device that can continuously read and record RF based communication at public places with high e-passport density like airports. The second one is a special-purpose hardware of reasonable price for fast cryptanalysis of symmetric ciphers. It consists of a reprogrammable machine COPACOBANA (Cost-Optimized Parallel Code Breaker), which is optimized for running crypt-analytical algorithms [13].

After the real-time decryption with our MRTD cracker, the plaintext information can be inserted into distributed databases. When such devices are installed in several different airports or used in other similar places, e.g., in trains, one is able to trace any individual similar to tracing packages sent using postal services such as UPS. This is an important issue since such databases when placed on the Internet can be used by anyone to trace a specific person. This information, however, can be exploited by criminals like terrorists or by detectives, data mining agencies, etc.

2 Overview of E-Passports

The International Civil Aviation Organization (ICAO) has issued specifications for Machine Readable Travel Documents (MRTDs) [20, 19, 16, 17, 14, 18] that are capable of including biometric data of the passport holder in machine readable form. Biometric data is stored on a contactless Integrated Circuit (IC) that is embedded in the (physical) passport document. Biometric data includes the facial image of the passport holder, which ICAO assesses not to be privacy sensitive information. Additional (optional) biometric data includes images of the finger(s) and iris of the passport holder. Both, digital fingerprints and digital iris scans are definitively privacy sensitive. For example, in Germany, it is planned to enforce the storage of digital fingerprints in e-passports from 2007 on [2].

The principles involved are the manufacturers, the personalization⁵ agent acting on behalf of the issuing state or organization, the rightful MRTD holder and control officers acting on behalf of the issuing and receiving state.

⁴ Experiments on the Netherlands' e-passport demonstrated that the encrypted information can be revealed in 3 hours after intercepting the communication [4, 23]. The issuing scheme in the Netherlands has about 35 bits of entropy [23]

⁵ The process by which the photo, signature and biographical data are applied to the document.

Control officers make use of an inspection system at border control. The inspection system is a terminal that is equipped with an RF reader device to carry out the RF based communication with MRTDs. During operational use, the players are the rightful MRTD holder, the control officers acting on behalf of the issuing and receiving state as well as other individuals, e.g., travellers and employees.

Referring to the German Protection Profile [5], four phases are defined for the life cycle of MRTDs: (1) Development Phase, (2) Manufacturing, (3) Personalization of the MRTD, and (4) Operational Use. Personalization of the MRTD and its environment are defined and controlled by the issuing state or organisation and are not covered by the evaluation and certification process. Note that this protection profile considers Basic Access Control, but not extended Access Control as, e.g, Active Authentication.⁶

In Germany, the validity of passports is 10 years and it is worth noting that the passport remains valid if the IC is defect.

2.1 Derivation of Basic Access Keys

Basic Access Control derives access keys from parts of the MRZ (Machine Readable Zone) that is printed in the MRTD physical document. These data are intended to be read only with agreement of the MRTD holder by inspection systems. Hereby, it is assumed that only the rightful MRTD holder and control officers read this visible information during lifetime of the document. Once, the MRZ is released, the MRTD holder loses control whether the MRZ data are further spread.

In detail, key derivation uses

1. the 9-digit alphanumeric passport `Document-Number`,
2. the `Date-of-Birth` of the MRTD holder and
3. the `Date-of-Expiry` of the MRTD document.

Each data item includes a check digit. For the computation of the check digits see [20, 24, 1]. These three items form an ASCII string `Document-Number || Date-of-Birth || Date-of-Expiry` (see [17]).

As it can be seen in Fig. 1, first K_{Seed} is derived as the most significant 16 bytes by using SHA-1. From K_{Seed} both an encryption key K_{ENC} and a MAC key K_{MAC} are obtained. For their key derivation, two different constants c are used: $c = '00000001'$ for K_{ENC} and $c = '00000002'$ for K_{MAC} . The most significant 16 bytes of the SHA-1 computation form the Triple-DES key of K_{ENC} and K_{MAC} , respectively.

⁶ References [5, 8, 9] even say that the MRTD allows the personalization agent to disable the Basic Access Control for use of the MRTD with Primary Inspection Systems, i.e., inspection systems may gain access to the logical MRTD contents without using Basic Access Control.

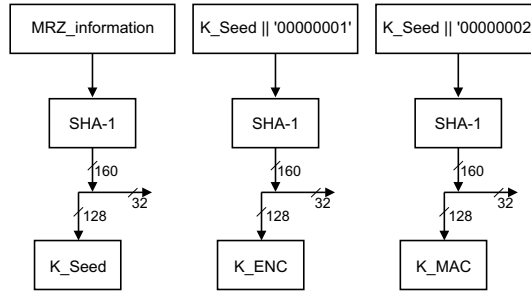


Fig. 1. Derivation of K_{Seed} and follow-up derivations of K_{ENC} and K_{MAC} from $MRZ_information := Document-Number || Date-of-Birth || Date-of-Expiry$.

Entropy of Basic Access Control keys: The entropy of the Basic Access Control keys depends on the passport numbering scheme of the issuing state. For example, Dutch Basic Access Control keys were reported to have only about 35 bits of entropy because of the dependency between expiration date and the serial passport number [23].

For German passports, a substantiated estimation on the entropy is not published, yet. Reference [11] estimates an entropy of 14 bits for the date of birth and an entropy of 11 bits for the date of expiry if the validity period spans 10 years⁷. Let H_{PN} be the entropy for the passport number that is estimated in more detail below. Assuming that the date of birth is an independent stochastic variable, the overall entropy H is bounded by $H_{PN} + 14 \leq H \leq H_{PN} + 25$. As the German scheme uses numeric characters only, the upper bound for H_{PN} is about 30 bits assuming no further knowledge on the passport number distribution scheme. However, it is known that the German passport number includes a four digit ‘Behördenkennzahl’ (BKZ), i.e., a number that belongs to the local issuing agency [3, 1]. Referring to [1] there are about 7000 local agencies in Germany, but not all have an individual BKZ. Cities with high population densities are assigned multiple subsequent BKZs. The four-digit BKZ is followed by a five-digit serial number. Due to the fact that system parameters such as the number of BKZs and the number of residents in each BKZ are not made publicly available, H_{PN} cannot directly be computed. In a rough demographic model we end up at an entropy of about 26 bits for H_{PN} in Germany, i.e., our estimation on the entropy of the German issuing scheme is $40 \leq H \leq 51$ considering a full roll-out of the system after 10 years.

So far, these estimations are conservative ones. One may break it down to significantly less entropy by making assumptions, e.g., one may assume that (1) the city of residence and (2) the date of birth of the individual to be tracked is known to the attacker. Further, one may assume that (3) one or more pairs of (passport number, passport expiry date) of the corresponding BKZ and (4)

⁷ As e-passports are in use in Germany since about half a year, current entropy yields 7 bits for date-of-expiry.

the overall number of residents of the corresponding BKZ is known to the attacker⁸. Then, depending on concrete assumptions, the remaining entropy may be reduced down below 20 bits.

Astonishingly, such estimations seem to be out of the scope of [8, 9] that certify a Strength of Mechanism of Sof-High⁹ for Identification and Authentication based on Challenge-Response and data exchange under secure messaging (see Subsect. 2.2). References [8, 9] note that the personalization agent in collaboration with the issuing state or organisation is responsible for providing keys with sufficient entropy. However, this is obviously not warranted by the German issuing scheme.

2.2 Key Agreement at Basic Access Control

Based on the access keys K_{ENC} and K_{MAC} , session keys are established using a three-pass authentication protocol with random numbers. The protocol runs between the RF reader that is part of the inspection system and the MRTD chip as shown in Fig. 2 (see also [17, 11]).

As result of Fig. 2, the session key KS_{Seed} is computed as $KS_{Seed} = K_{IFD} \oplus K_{ICC}$. By using the same key derivation scheme as in Section 2.1, Triple-DES session keys KS_{ENC} and KS_{MAC} are obtained. The subsequent communication transfers logical MRTD data and is secured with these Triple-DES session keys KS_{ENC} and KS_{MAC} . We denote the overall set of communication data on the wireless channel with C .

3 Our Attacks On Privacy

We present two attacks on privacy: (1) Direct key search with a proprietary RFID reader targeting MRTDs (Subsect. 3.1) and (2) Eavesdropping during a Basic Access Control protocol run with a regular inspection system and subsequent key search (Subsect. 3.2 and Subsect. 3.3). Both attacks can be drastically speed-up by inserting prior knowledge about the MRTD holder.

As consequence of successful attacks, distributed databases may be deployed for tracing citizens once their MRTD identification data is revealed.

3.1 Direct Key Search

We assume that the adversary does not know the entire MRZ information. However, the adversary may know or guess on the date-of-birth and also on the

⁸ Think of many hotels, banking companies and postal offices that require a copy of the passport of their clients. Further, databases of many companies already include security sensitive data such as date of birth and residence of their clients and employees.

⁹ A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing an high attack potential.

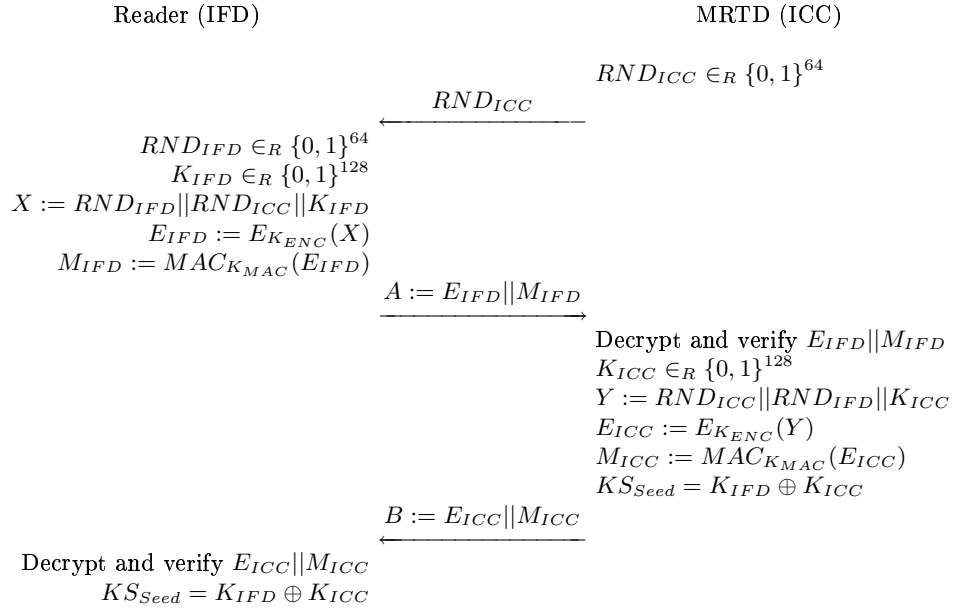


Fig. 2. Basic Access Control Protocol between the RF reader (also referred to as Interface Device IFD) and the MRTD chip (also referred to as Integrated Circuit Card ICC). E denotes Triple-DES encryption, MAC denotes the cryptographic checksum according to ISO/IEC 9797-1 MAC Algorithm 3 [17].

city of residence of individuals¹⁰. The adversary owns an RF reader device and is able to position it near-by to the MRTD holder, e.g., in crowded public areas. As shown in Fig. 2, the Basic Access Control protocol is stopped by the MRTD if $E_{IFD} || M_{IFD}$ is not verified. Note that MRTD does not implement a failure counter, i.e., MRTD is not blocked as result of many unsuccessful protocol runs¹¹. If the MRTD sends a response $E_{ICC} || M_{ICC}$, this, however, implies that the guess on the Basic Access Control keys is most likely correct. Given the Basic Access Control keys, the adversary knows the established session keys for the secured communication link. The adversary now acts similarly to a proper reader device of an inspection system and actively retrieves logical MRTD data via the secured communication link.

¹⁰ For example, if the attack is mounted in Cologne, it is probable to interfere with many people from Cologne.

¹¹ However, as a countermeasure against direct key attacks artificial delays may be implemented once a protocol run is stopped.

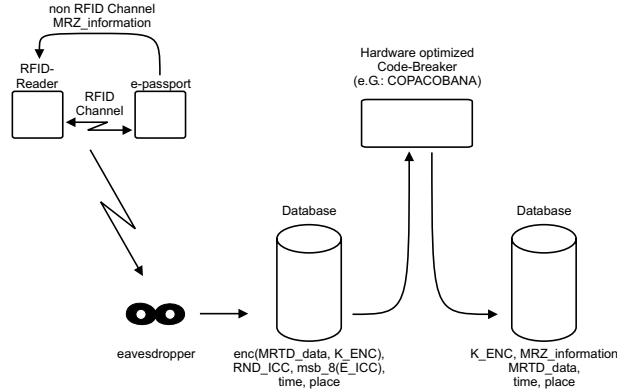


Fig. 3. Overview of the system setup to enable tracing activities.

3.2 Eavesdropping at an Inspection System

We assume an adversary succeeds to monitor the communication of the Basic Access Control protocol between a MRTD and an inspection system shown in Fig. 2. This is a realistic assumption, if the adversary is within a distance of a few meters [23, 6]. Especially, if controls are carried out in a train, this is usually the case. By assumption, the adversary does not know the MRZ information. Nevertheless, the adversary may be able to guess the date-of-birth of the MRTD holder. Further, the adversary may identify the issuing state of the MRTD document and may know its distribution scheme of passport numbers.

The adversary monitors RND_{ICC}, A and B of Fig. 2 and the entire subsequent secured communication C .

3.3 Subsequent Key Search

After obtaining the protocol data of Subsect. 3.2, the adversary runs a key search on the MRZ information to find a match to the most significant eight bytes of E_{ICC} (see Fig. 2, part of B) during the protocol run. More concretely, the adversary computes $E^* = E_K(RND_{ICC})$ where K denotes possible candidates for K_{ENC} and E denotes Triple-DES encryption. If $msb_8(E_{ICC}) \stackrel{?}{=} E^*$, C can be decrypted and the logical MRTD data are revealed.

As described in Section 2.1, key derivation of K_{ENC} requires two SHA-1 computations. SHA-1 computations are less efficient in hardware so that it would be convenient to pre-compute K_{ENC} candidates in a database. Because of this, we distinguish two different architectures for an MRTD cracker.

Architectures with and without Pre-Computing In case of a low-entropy issuing scheme it is convenient to pre-compute K_{ENC} in a database indexed by date-of-birth and/or residence. If the overall entropy is in the order of 35, the

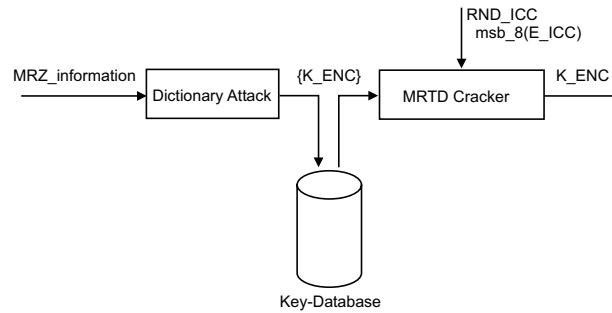


Fig. 4. MRTD cracker using precomputation of K_{ENC} . The MRTD cracker has to implement Triple-DES only.

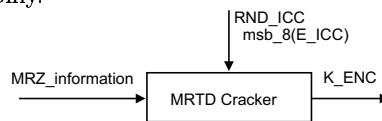


Fig. 5. MRTD cracker without precomputation of K_{ENC} . The MRTD cracker has to implement both SHA-1 and Triple-DES.

entropy per date of birth is in a rough estimation reduced to about 21. Storage complexity per date of birth then is about 33.6 MB and per year of birth about 12.2 GB. Depending on the most probable age of the MRTD holder and/or the most probable residence, precomputed database entries K_{ENC} can be directly fed into the MRTD cracker engine.

In case of an issuing scheme entropy of about 50, the entropy per date of birth is in a rough estimation reduced to about 36. Precomputing would require a storage capacity of 1.1 TB per date of birth and is – even on distributed systems – hardly feasible for low or medium costs. Furthermore, time-memory attacks using Triple-DES only are not appropriate, as only a small fraction of the entire Triple-DES key space has to be searched. Here, the hardware cracker probably has to include both SHA-1 and Triple-DES.

3.4 Distributed Databases – Vision of Basic Access Control Privacy

Once the key K_{ENC} is found, the session keys of Basic Access Control can be derived and the logged communication data C can be decrypted. Thus the adversary reveals personal data of the passport holder, such as name, date of birth, sex, validity, document number, issuer, the complete MRZ information and a picture of the card holder in digital form.

These personal information can be fed into distributed databases all over the world, thus anybody searching for a specific person, is able to track the

person at public places¹². Tracking may be done by loading the key K_{ENC} of the individual to be tracked into operational MRTD crackers or by operating RF readers at public places and performing a direct key search. If established, these databases can be updated with recent places visited and may achieve a state that is similar to publishing flight passenger lists and similar to what is already easily possible for issuing and receiving states.

4 Our Device Architectures

4.1 RF Eavesdropper

Referring to Subsect. 3.2, the communication with e-passports has to be monitored in public places, e.g., at border control. For ISO 14443 RFID communication the distance between the reader and the tag¹³ is specified to be smaller than 15 cm. This constraint is caused by the fact, that the reader has to transmit the operating power to the RFID tag by a magnetic field. However, the electromagnetic waves during the communication exceed this specified distance and can be observed at a much higher distance (detailed below).

For the RFID-communication two different channels are used:

- Reader to Tag: This channel has to provide the tag with energy and has to send information from the reader to the tag. The reader generates an electromagnetic field with the frequency 13.56 MHz. This field provides the tag with energy. To transmit data to the tag the field is switched off for a short period using a modified Miller code [7].
- Tag to Reader: The tag sends data to the reader by modifying its own load. In ISO 14443 it is specified that the tag uses 848 kHz load modulation. The information is transferred using the Manchester code [7].

Eavesdropping Hardware The signal from the reader to the tag is about 80 dB stronger [7] than the load modulation signal which is used for communication on the backwards channel. Therefore, it is more difficult to observe the data sent from the MRTD ICC than the data which the reader sends to it, because the more powerful signal from the reader suppresses the weak signal generated by the MRTD ICC.

As the tag uses 848 kHz load modulation, the signal generated by the tag is placed in side-bands of the carrier frequency generated by the reader. The resulting frequency caused by this load modulation is $13.56 \text{ MHz} \pm 848 \text{ kHz}$, i.e. around 12.7 and 14.4 MHz.

¹² Note that, e.g., German law [3] prohibits from using the serial passport number and personal passport data for automated storage and retrieval, but German law does not avenge such offences, if committed abroad.

¹³ In this Subsection we also use tag as a synonym for e-passport, respectively, for MRTD ICC.

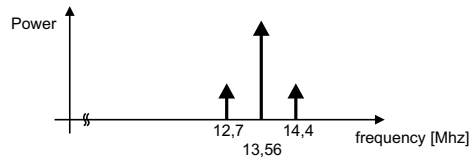


Fig. 6. RFID-Signal-Spectrum

A simple eavesdropping approach is to set up an antenna for the frequency 13.56 MHz. For such an antenna an important parameter is the gain that describes how much power the antenna receives in the main direction compared to the power which is received by a reference antenna for the operating frequency. For eavesdropping purposes, one would use an antenna with a high gain, which results in a highly directional characteristic. Further, to increase the distance for observing the RFID communication an additional amplifier to strengthen the received signal is useful.

As both signals (from MRTD ICC and from the reader) are signals with the base frequency 13.56 MHz the same antenna setup can be used for both directions, so that only one antenna is needed. To obtain the transferred data between tag and reader the received signal has to be analyzed. To retrieve the modified Miller code the 13.56 MHz signal has to be detected. This can simply be done by using an 13.56 MHz envelope detector at the antenna amplifier output. To retrieve the Manchester code sent from the tag it is necessary to detect the 848 kHz load modulation. Previous experiments showed [6], that this can be done by tuning the whole system to one of the side-bands 12.7 MHz or 14.4 MHz.

Actually, we consider the usage of a PLL¹⁴ and a frequency mixer as shown in Fig. 7. The advantage of this setup is an extension of the operating range because both, the upper and the lower side-bands, are detected.

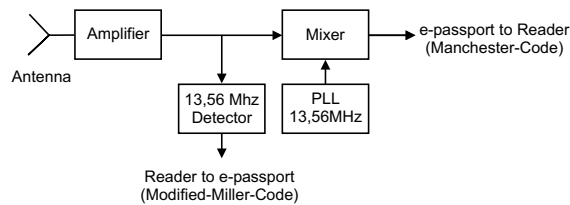


Fig. 7. Use of a PLL and a frequency mixer for signal preparation.

Experiments with a simple setup have already shown [6], that without optimizing antenna and amplifier the communication can be easily monitored from a distance of 2 metres using an antenna tuned on one side-band. We expect

¹⁴ Phase Locked Loop

that by optimizing the setup, using a PLL-Mixer Setup, distances up to several metres can be reached.

Another recent work by Hancke [10] practically demonstrated that the two-way communication between the reader and tag can be intercepted from 4 metres. Further, [10] states that it is very feasible that this distance can be increased, e.g., with application specific antennas and more complex signal processing.

4.2 MRTD Cracker

Cryptanalysis of modern cryptographic algorithms has been a subject of research for many years. Much effort has been put into breaking ciphers by different cryptanalytic methods and distributed search algorithms. A common characteristic of many distributed cryptanalytical algorithms is high parallelism. A way of implementing such algorithms is to perform the required operations by means of hardware modules, however, at reasonable costs. Basically, for the purpose of security the computation effort of cryptanalysis should be high, e.g., in the order of 2^{80} operations.

A software approach of distributed computing with loosely coupled processors is one possible implementation choice for an MRTD cracker. For instance, the SETI@home project [25] is based on using the idle cycles of the huge number of computers connected via the Internet. The results of this approach have been quite successful for selected problems which are not viable with the computing power within a single organization. Using distributed computing, however, requires the corresponding infrastructure to solve the underlying problem, and trust in the computing nodes.

Special-purpose hardware is an alternative choice, especially at exhaustive key search for the Data Encryption Standard (DES) [15]. A brute-force attack of this type is more than two orders of magnitude faster when implemented on Field Programmable Gate Arrays (FPGA) than in software on general purpose computers at equivalent costs¹⁵. If performance is the most important criterion for an MRTD cracker, an ASIC design is the method of choice. A drawback may be the high non recovering engineering costs. However, with the recent advent of low-cost FPGA families with much logic resources, they provide a promising alternative tool for the high computational effort required for cryptanalytic applications. In addition to the cost advantage over PC-based machines, such a machine has the advantage over ASIC-based designs that it can be used to attack various different cryptosystems without the need to rebuild a new machine each time.

For our purposes we make use of COPACOBANA, which is an optimized hardware architecture for breaking codes. The architectural concept and the realization of COPACOBANA, consisting of a backplane, 20 FPGA DIMM modules, and a controller card can be found in [13]. For the use as a MRTD cracker

¹⁵ As mentioned in [13], a single FPGA at a cost of 40 Euro (current market price) can test 400 million keys per second, a PC (Pentium4, 3GHz) for 200 Euro checks 2 million keys per second. Hence, 5 FPGAs can perform the same task approximately 1000 times faster than a PC at the same cost.

a variant of COPACOBANA has to be developed that makes use of onboard DRAM memory for the storage of the precomputed candidate values of K_{ENC} (refer to Subsect. 3.3 for the discussion on precomputation). The estimates of the expected capabilities of the completely configured COPACOBANA are to test $1.2 \cdot 10^{10}$ blocks of Triple-DES per second which corresponds to searching a key subspace of about 2^{33} per second [21].

5 Conclusion

Whereas strong cryptographic mechanisms for authenticity are specified for MRTDs, the mechanisms for access control and confidentiality are still weak. MRTD issuing states seem not to care thoroughly about privacy needs – or said differently – enable that third parties mount global traceability systems.

References

1. Behördenkennzahl. <http://www.pruefziffernberechnung.de/Begleitdokumente/BKZ.shtml>.
2. Häufig gestellte Fragen. <http://www.bsi.bund.de/fachthem/epass/faq.htm>.
3. Paßgesetz PaßG. http://www.gesetze-im-internet.de/bundesrecht/pa_g_1986/gesamt.pdf.
4. Privacy issues with new digital passport. <http://www.riscure.com/news/passport.html>.
5. Common Criteria Protection Profile, Machine Readable Travel Document with "ICAO application", Basic Access Control, BSI-PP-0017, 2005. <http://www.bsi.bund.de/zertifiz/zert/reporte/PP0017b.pdf>.
6. Thomas Finke and Harald Kelter. Radio Frequency Identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems. http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf.
7. K. Finkenzeller. *RFID-Handbuch*. Hanser Fachbuchverlag, Third edition, October 2002.
8. Bundesamt für Sicherheit in der Informationstechnik. BSI-DSZ-CC-0316-2005 for TCOS Passport Version 1.01 / P5CT072 and TCOS Passport Version 1.01 / SLE66CLX641P from T-Systems International GmbH Service Line SI, 2005. <http://www.bsi.bund.de/zertifiz/zert/reporte/0316a.pdf>.
9. Bundesamt für Sicherheit in der Informationstechnik. BSI-DSZ-CC-0362-2006 for TCOS Passport Version 1.0 Release 2 / P5CD072V0Q and TCOS Passport Version 1.0 Release 2 / SLE66CLX641P/m1522-a12 from T-Systems Enterprise Services GmbH SSC Testfactory & Security, 2006. <http://www.bsi.bund.de/zertifiz/zert/reporte/0362a.pdf>.
10. Gerhard P. Hancke. Practical Attacks on Proximity Identification Systems (Short Paper). In *IEEE Symposium on Security and Privacy 2006*, 2006. <http://www.cl.cam.ac.uk/~gh275/SPPractical.pdf>.
11. A. Juels, D. Molnar, and D. Wagner. Security and privacy issues in e-passports. In *SecureComm 2005, First International Conference on Security and Privacy for Emerging Areas in Communication Networks, Athens, Greece*, September 2005.

12. G.S. Kc and P.A. Karger. Security and Privacy Issues in Machine Readable Travel Documents (MRTDs). RC 23575, IBM T. J. Watson Research Labs, April 2005.
13. Sandeep Kumar, Christof Paar, Jan Pelzl, Gerd Pfeiffer, Andy Rupp, and Manfred Schimmler. How to Break DES for € 8,980. In *SHARCS'06 – Special-purpose Hardware for Attacking Cryptographic Systems*, pages 17–35, 2006. http://www.hyperelliptic.org/tanja/SHARCS/talks06/copa_sharcs.pdf.
14. ICAO TAG MRTD/NTWG. Biometrics Deployment of Machine Readable Travel Documents, Technical Report, 2004. <http://www.icao.int/mrtd>.
15. NIST FIPS PUB 46-3. *Data Encryption Standard*. Federal Information Processing Standards, National Bureau of Standards, U.S. Department of Commerce, January 1977.
16. International Civil Aviation Organization. Annex I, Use of Contactless Integrated Circuits In Machine Readable Travel Documents, 2004. <http://www.icao.int/mrtd>.
17. International Civil Aviation Organization. Machine Readable Travel Documents, PKI for Machine Readable Travel Documents offering ICC Read-Only Access, 2004. <http://www.icao.int/mrtd>.
18. International Civil Aviation Organization. Machine Readable Travel Documents, Technical Report, Development of a Logical Data Structure - LDS For Optional Capacity Expansion Technologies, 2004. <http://www.icao.int/mrtd>.
19. International Civil Aviation Organization. Machine Readable Travel Documents, Supplement to Doc9303-part1-sixth edition, 2005. <http://www.icao.int/mrtd>.
20. International Civil Aviation Organization. Machine Readable Travel Documents, Doc 9303, Part 1 Machine Readable Passports, Fifth Edition, 2003.
21. Jan Pelzl. Personal Communication.
22. Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. The Evolution of RFID Security. *IEEE Pervasive Computing*, 5(1):62–69, 2006.
23. Harko Robroch. ePassport Privacy Attack, Presentation at Cards Asia Singapore, April 26,2006. <http://www.riscure.com>.
24. Alan De Smet. Machine Readable Passport Zone. <http://www.highprogrammer.com/alan/numbers/mrp.html>.
25. University of California, Berkeley. Seti@Home Website, 2005. <http://setiathome.berkeley.edu/>.