Speedup for European ePassport Authentication

Roel Peeters, Jens Hermans, Bart Mennink
KU Leuven, ESAT/COSIC and iMinds
firstname.lastname@esat.kuleuven.be

Abstract: The overall ePassport authentication procedure should be fast to have a sufficient throughput of people at border crossings such as airports. At the same time, the ePassport and its holder should be checked as thoroughly as possible. By speeding up the ePassport authentication procedure, more time can be spend on verification of biometrics. We demonstrate that our proposed solution allows to replace the current combination of PACE and EAC with a more efficient authentication procedure that provides even better security and privacy guarantees. When abstracting away from the time needed for the ePassport to verify the terminal's certificate, a speed-up of at least 40% in comparison with the current ePassport authentication procedure is to be expected.

1 Introduction

Part of the ePassport authentication is run on an RFID chip contained within the ePassport. This means that when designing ePassport authentication protocols, one needs to take into account efficiency and cost constraints on the chip side. At the same time, the overall ePassport authentication procedure, including the verification of biometrics of the ePassport holder, should ideally take less than ten seconds to reach a sufficient throughput of people at border crossing such as airports, without compromising on security. Therefore it is important, that newly proposed solutions are at least as efficient as the current solution when providing improved security features or more efficient when providing at least the current security features. Additionally, to keep the cost low, the newly proposed solutions should also be able to run on the currently available hardware.

Recently a couple of ePassport authentication improvements were proposed. Bender *et al.* [BFK13] proposed to combine password authenticated connection establishment (PACE)[1] with active authentication (AA), which results in a cost reduction on the tag side by one elliptic curve multiplication: 6 elliptic curve multiplications instead of a total of 7 for PACE and AA separately. However, this improvement only applies to the version of PACE with the generic mapping and not to the version with the integrated mapping, where the total for PACE and AA separately would be 4 elliptic curve multiplications. Buchmann *et al.* [BPBP13] propose an improved BioPACE protocol where the ePassport holder's biometrics are used in combination with a biometric template protection scheme as input for PACE instead of the ePassport's Machine Readable Zone (MRZ). This bypasses the need for extended access control (EAC) which is aimed at limiting access to the sensitive data

[1] An overview of these protocols is given in Sect. 2

stored on the ePassport such as biometrics. Note that this improved BioPACE protocol does not provide protection against chip cloning and as such requires either AA or chip authentication to take place afterwards. Additionally, it has as drawback that an active adversary with access to the ePassport could use it to derive information about the biometrics of the ePassport holder.

When verifying a European ePassport, one needs to make a distinction between two situations:

1. The verifier wants access to the sensitive data stored on the ePassport, which are protected by extended access control such as biometrics (fingerprints, iris); there is support on the verifying terminal for EAC; and the ePassport's issuing country granted the inspection systems of the verifying country access to the sensitive data protected by EAC.
2. The verifier does not want access to the protected biometric data; there is no support on the verifying terminal for EAC; or the ePassport's issuing country did not grant inspections systems of the verifying country access to data protected by EAC.

Our proposal only applies to the former situation and hence we will only discuss this situation throughout the paper. To handle the latter situation, ePassports will still need to support basic access control (BAC)/PACE to read out basic information that is stored on the ePassport, passive authentication to ensure the authenticity of the read-out data, and active authentication/chip authentication to protect against chip cloning.

Concretely, our contributions are as follows:

- In Sect. 2, we give an overview of the current ePassport authentication procedure and its properties in terms of security and privacy.
- We propose to replace the current combination of PACE and EAC protocols with a more efficient authentication procedure that relies on a single authentication protocol in Sect. 3. For the underlying authentication we choose on widely studied SIGMA-I protocol [Kra03] and proposed a new protocol IBIHOP+, which builds upon the IBIHOP protocol [PHF13]. Both protocols can be realized on the current ePassport chips.
- In Sect. 4 we evaluate our proposed solution for the two protocols and compare these with the current ePassport authentication solution in terms of security, privacy, efficiency and implementation considerations. We show that both our proposed solution achieves better security and privacy properties and moreover is more efficient in the number of communication rounds. For the newly proposed IBIHOP+ we additionally show a reduction in the number of computations at the chip side.

2 Current Situation

Current European biometric-enabled ePassports allow access to basic information to terminals to successfully complete the PACE protocol [BSI10] with the chip. To be compliant with International Civil Aviation Organization (ICAO) regulations, there is also support for the weaker BAC protocol [ICA06] that also allows access to this basic data. However, BAC is expected to be replaced by the PACE-based supplemental access control (SAC) protocol by 2018 [ICA13]. For access to the sensitive data, such as biometrics, European ePassports require EAC[2]. These implement EAC version 1 [BSI10], which consists of first chip authentication and then terminal authentication and requires passive authentication to have taken place before chip authentication. Figure 1 depicts the current European ePassport authentication process, where PACE takes place first and is followed later on by EAC.

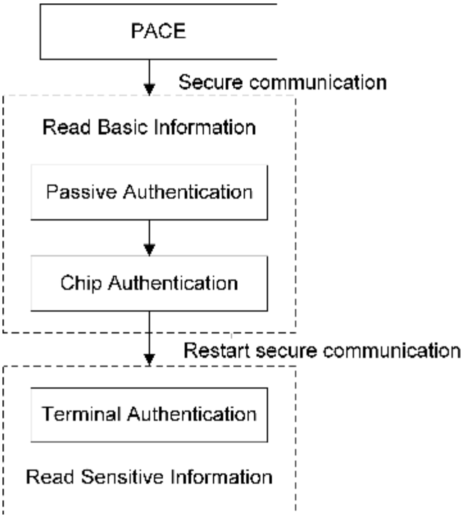

Figure 1: Current ePassport authentication procedure.

PACE provides forward secure key agreement based on a shared key between the ePassport and the terminal, *e.g.*, the MRZ of the ePassport. This agreed key will be used for setting up a secure communication channel. Over this secure communication channel, the basic information of the ePassport is read out. There exist two versions of PACE, because the designers also considered the cost of implementation. The first version of PACE uses a so-called generic mapping and relies on two consecutive Diffie-Hellman key exchanges. The second makes use of an integrated mapping for which the first Diffie-Hellman key exchange is replaced by a symmetric-key cryptographic solution, reducing the number of costly elliptic curve operations by 2 elliptic curve multiplications. Note that the security evaluation of PACE given by Bender *et al.* [BFK09] only applies to the version with generic mapping.

[2] This is mandatory *cfr.* European Commission Decision C(2006) 2909 of 28 June 2006.

Over this secure authentication channel, we continue the ePassport authentication process. Performing passive authentication (verifying the read out basic data) is mandatory before chip authentication can take place. After chip authentication, secure communication is restarted and finally terminal authentication is performed. Upon the chip accepting the terminal, the sensitive data can be communicated to the terminal.

Properties

We will define the security and privacy properties on the RFID chip in accordance with the latest RFID privacy model by Hermans *et al.* [HPP14]. This model builds further upon the generally accepted RFID privacy model of Hermans *et al.* [HPVP11], with added support for multiple readers and two new attacker classes to cover insider attacks. To fulfill the same requirements as the combination of PACE and EAC, one needs to provide at least:

- Wide-destructive privacy [HPP14]: for an adversary with the power to modify the exchanged messages between ePassports and a terminal, with full control over an ePassport of his own, and able to observe the outcome (success or failure), it should be hard, when not knowing a unique identifier of the ePassport under attack such as the MRZ when the messages are exchanged, to link a protocol run to a specific ePassport. This is similar to resistance against offline guessing property of PACE, with the difference that we now also allow active attacks.
- Extended soundness [HPP14]: the ePassport should be able to securely authenticate to a terminal without leaking information to the terminal that would allow the terminal to authenticate to another terminal as being the ePassport. This is referred to as protection against chip cloning, which is both provided by chip authentication as active authentication.
- Extended soundness for terminal authentication: similar to extended soundness but specific for terminal authentication.
- Mutual authentication: chip and terminal authentication should be linked together.
- Key agreement with forward secrecy: to securely exchange subsequent data between ePassport and terminal, which will remain confidential even when the private key of the terminal leaks at some point in the future.

Of lesser importance (as discussed in Sect. 4), the current combination of PACE and EAC also provides:

- Preventing challenge semantics because the transcripts produced by the protocol are non-transferable (EAC).
- Verification that the terminal has physical access to the ePassport's data page (PACE).

3 Proposed Solution

Instead of bootstrapping from a low entropy value printed on the ePassport, *e.g.,* MRZ, we propose to directly use a strong mutual authentication protocol. To safeguard the citizen's privacy, strong terminal authentication should take place first. Then, after the ePassport verifies the terminal's authentication, the ePassport will authenticate privately to this terminal. We selected two efficient protocols that follow this pattern, namely Sigma-I [Kra03] and IBIHOP [PHF13], which will be discussed in more detail below. Both protocols can be implement on the current ePassports' chips[3].

Please note that terminal authentication in itself is not enough, the ePassport also needs to be ensured that the terminal is authorized by the issuing country to read out the (sensitive) data. To this end, the terminal will first need to get the issuing country from the MRZ and then provide the correct terminal certificate, as is the case for terminal authentication as specified by BSI [BSI10]. After the terminal certificate has been verified, one of the two following protocols is run, where the ePassport takes the public key of the terminal from the validated terminal certificate. Likewise, the terminal needs to be sure that the public key of the ePassport is certified by the ePassport's issuing country. Therefore, passive authentication will take place after one of the two protocols has been successfully executed. The general ePassport authentication procedure is depicted in Fig. 2.

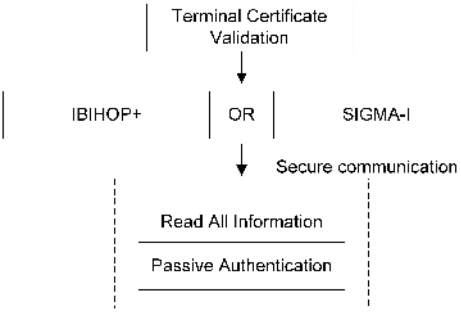

Figure 2: Alternative ePassport authentication procedure.

3.1 Sigma-I

Krawczyk [Kra03] proposed several Sigma protocols of which Sigma-I is of particular interest. This protocol, which is depicted in Fig. 3, allows the ePassport to only send out his identifiable information after having authenticated the terminal. As already suggested by Krawczyk, we use an authenticated encryption scheme to optimize the protocol. We selected Schnorr's signature scheme [Sch91] because of its security and high efficiency. Generating a signature takes one elliptic curve multiplication, while verifying takes two elliptic curve multiplications and one elliptic curve addition.

[3] Authenticated encryption call always be implemented by using a generic Encrypt-then-MAC construction[BN00].

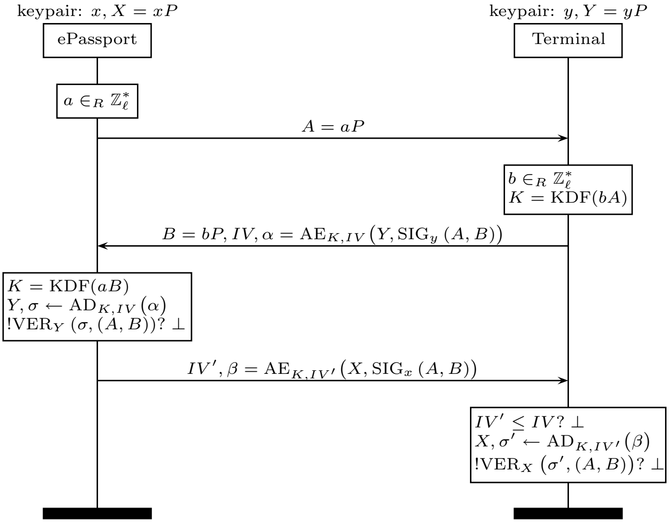
keypair: $x, X = xP$
ePassport
keypair: $y, Y = yP$
Terminal
$a \in_R \mathbb{Z}_\ell^*$
$A = aP$
$b \in_R \mathbb{Z}_\ell^*$
$K = \text{KDF}(bA)$
$B = bP, IV, \alpha = \text{AE}_{K,IV}\big(Y, \text{SIG}_y\ (A, B)\big)$
$K = \text{KDF}(aB)$
$Y, \sigma \leftarrow \text{AD}_{K,IV}\ (\alpha)$
$!\text{VER}_Y\ (\sigma, (A, B))?\ \perp$
$IV', \beta = \text{AE}_{K,IV'}\big(X, \text{SIG}_x\ (A, B)\big)$
$IV' \leq IV?\ \perp$
$X, \sigma' \leftarrow \text{AD}_{K,IV'}\ (\beta)$
$!\text{VER}_X\ (\sigma', (A, B))?\ \perp$

Figure 3: The Sigma-I protocol [Kra03].

3.2 IBIHOP

Peeters *et al.* [PHF13] proposed IBIHOP, which is depicted in Fig. 4. It is important to mention that one of this protocol's design goals was to be very space-efficient (minimal circuit area) on RFID tags, hence it does not make use of hash functions or authenticated encryption and only used the x-coordinates of points on the elliptic curve. This protocol provides wide-strong ePassport privacy and tag-first mutual authentication with extended soundness for both ePassport as terminal authentication. The protocol's high efficiency is due to the fact that it is designed for efficient mutual authentication and not for key agreement. Even though mutual authentication implies key agreement, both parties can easily derive a key $K = \text{KDF}(e, yR = rY, X)$, this does not provide forward security. An adversary obtaining the private key of the terminal y, can reconstruct this key for any past exchange of messages between an ePassport and the terminal. Given R_i, f_i, s_i and y, the key K_i can be reconstructed as follows: let $e_i = f_i - [yR_i]_x$ and $K_i = \text{KDF}(e_i, yR_i, e_i^{-1}(s_iP - R_i))$.

We propose a new variant of the IBIHOP protocol, IBIHOP+ (see Fig. 5), to also include forward secure key agreement. For forward key agreement, we introduce a full Diffie-Hellman key agreement with fresh randomness provided by the two parties, resulting in one more elliptic curve multiplication. By introducing a hash function (which is already implemented on the ePassport chip and hence does not result in additional required circuit area), we will try to keep IBIHOP's original efficiency in number of operations on the elliptic curve: as such we will explicitly bind e and R_1 together with the authentication of the terminal at negligible cost. This makes that the first half of the security proof (mutual authentication), based on matching conversations until the third message still holds. Only the last message will be sent over an authenticated channel, in order to prevent an adversary to uniquely identify the ePassport later on, in the event the terminal's private key gets compromised. For the security proof, an adversary could be given access to K without it gaining any advantage towards breaking the security game. As such, the second part of the original security proof also holds. Similarly, the original proof for wide-strong privacy holds, when allowing the adversary access to K.

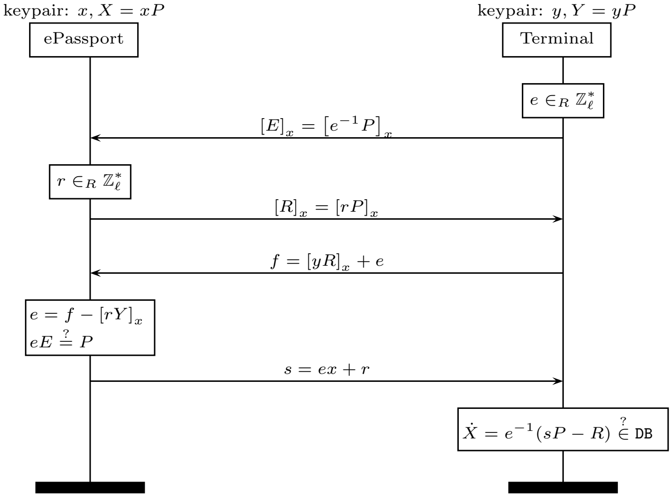

Figure 4: The IBIHOP protocol [PHF13].

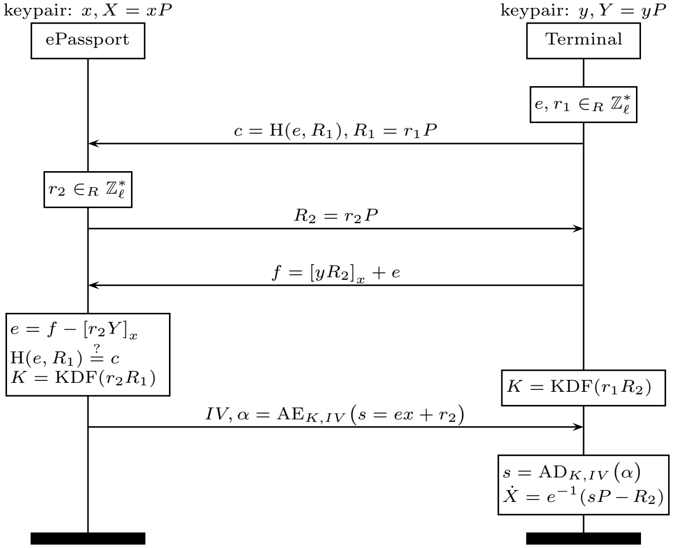
keypair: $x, X = xP$
ePassport
keypair: $y, Y = yP$
Terminal
$e, r_1 \in_R \mathbb{Z}_\ell^*$
$c = \mathrm{H}(e, R_1), R_1 = r_1 P$
$r_2 \in_R \mathbb{Z}_\ell^*$
$R_2 = r_2 P$
$f = [yR_2]_x + e$
$e = f - [r_2 Y]_x$
$\mathrm{H}(e, R_1) \stackrel{?}{=} c$
$K = \mathrm{KDF}(r_2 R_1)$
$K = \mathrm{KDF}(r_1 R_2)$
$IV, \alpha = \mathrm{AE}_{K,IV}(s = ex + r_2)$
$s = \mathrm{AD}_{K,IV}(\alpha)$
$\dot{X} = e^{-1}(sP - R_2)$

Figure 5: IBIHOP+ : our proposed IBIHOP variant with forward-secure key agreement.

4 Evaluation

4.1 Security and Privacy

Both proposed protocols (SIGMA-I and IBIHOP+) are proven to be wide-strong private, as opposed to PACE's attributed wide-destructive privacy[4]. Wide-strong private is the strongest privacy property which means that even when the adversary has all secret information stored on the chip, it will still not be able to tell a future protocol run of this chip apart from any other valid protocol run. Hence it is hard (in the security parameter ℓ of the used underlying curves) to trace even a single ePassport.

When also considering active attacks, the effective privacy offered by PACE is depending on the entropy h of the passwords used as its input, which is typically the machine readable zone (MRZ) of the passport. According to ICAO [ICA06] the maximum entropy provided by a MRZ for a ePassport with 10 year validity is 56 bit. However, it has been shown that the entropy can be reduced further for among others Belgian [AKQ08] ePassports: 38 bit, 23 bit when the date of birth is known; Dutch [HHJ$^+$08] ePassports: 50 bit, 41 bit when the age can be guessed correctly within a 5 year interval; and German [CLRPS07] ePassports: 40 bit. Note that it is easy to mount active attacks against ePassports since PACE does not provide reader authentication. A successful attack, with probability of at least $1/2^{56}$, will give the adversary access to the basic information, stored on the ePassport, that uniquely identifies the citizen. However, it remains impossible to read the sensitive information contained within the ePassport due the security of extended access control mechanism.

Both SIGMA-I and IBIHOP+ provide reader-first mutual authentication with strong ePassport and strong terminal authentication, where no identifiable information of the tag is shared before the reader strongly authenticated to the tag. As discussed in [PHF13], this is both an advantage for tag privacy and security, since the adversary is limited by not being able to send arbitrary formatted messages to the tag, only messages from a genuine reader will be accepted. The order in which mutual authentication takes place has also an effect on the need to prevent challenge semantics, as already informatively argued in [BSI10]. By having the reader authenticate first, the worst case scenario in which challenge semantics are not restricted to authorized terminal is avoided. However, if one is to insist on avoiding challenge semantics, only IBIHOP+ remains. The authentication in IBIHOP+ is not transferable since a terminal with private key y can always generate a valid transcript for an ePassport with a given public key X as follows:

- Pick the values e and s at random in $\mathbb{Z}_\ell$.
- Compute R_2 as $sP - eX$.

When considering the influence of compromise of the ePassport or the terminal on prior communications, the forward secrecy property of the key agreement is important. For the combination PACE + EAC, both PACE and chip authentication provide forward secrecy.

[4] PACE is definitely not wide-strong private, since an active attacker can always see if a protocol run corresponds with a given secret.

SIGMA-I and IBIHOP+ also provides forward secrecy. All these protocols prevent that an adversary can read the exchanged information or even identify ePassports used with this terminal, prior to compromise. After compromise of a terminal that is still authorized, the PACE protocol ensures that the data on the ePassport are better protected, because the terminal needs the password on the printed passport in order to be able to access the information the ePassport (and hence cannot read out any closed ePassport book). However, the proposed protocols can easily be adapted to provide similar protection by adding an extra round of communication in the end, where the terminal sends the read-out password over the secure connection. The chip then verifies the received password before allowing access to the data on the ePassport. By transferring the password after private mutual authentication took place, over the freshly established secure channel, we avoid weakening the privacy guarantees towards third parties given by the proposed protocols.

Table 1 gives an overview of the achieved security and privacy properties, as defined in Sect. 2, for the different ePassport authentication solutions.

Table 1: Security and privacy of different ePassport authentication solutions.

	PACE + EAC	SIGMA-I	IBIHOP+
Privacy (tracebility)	wide-destructive (1^h)	wide-strong (1^ℓ)	wide-strong (1^ℓ)
Privacy (data)	basic info (1^h)	basic info (1^ℓ)	basic info (1^ℓ)
	sensitive info (1^ℓ)	sensitive info (1^ℓ)	sensitive info (1^ℓ)
Extended soundness			
ePassport	yes	yes	yes
terminal	yes	yes	yes
Mutual authentication	tag-first	reader-first	reader-first
Key agreement	forward secrecy	forward secrecy	forward secrecy
Prevent challenge semantics	yes	no, but limited to authorized terminals	yes
Verify physical access terminal	yes	optional, + 1 round of communication	optional, + 1 round of communication

(1^h) in the password entropy (1^ℓ) in the security parameter

4.2 Efficiency

This comparison in Table 2 does not take into account passive authentication and the fetching and verifying of the terminal certificate (part of terminal authentication for EAC, terminal certificate validation for the proposed alternatives), which are needed in all cases. Computation-wise, only the more involved public key cryptographic operations are considered, while the less involved symmetric key cryptographic operations are neglected[5].

Our alternative solution, for both proposed authentication protocols, requires significantly less rounds of communication in comparison with PACE and EAC. Moreover, IBIHOP+ also requires fewer elliptic curve operations. We assume that the possible slight overhead

[5] If one were to count the symmetric operations for the combination of PACE and EAC, one also needs to take into account the additional operations needed to send data over a secure communication channel.

in computations on the terminal for our proposed alternative solution will not play a big part as terminals are expected to be fundamentally more powerful than the chip inside ePassports. Depending on the cost of communication versus computation on the chip, the expected speed-up will be at least 40 % (only taking computation into account) when using IBIHOP+ instead of the combination of PACE and EAC.

Table 2: Efficiency of different ePassport authentication solutions.

	PACE + EAC	SIGMA-I	IBIHOP+
ePassport computation	5 (+2)* ECmul 1 ECadd	5 ECmul 1 ECadd	3 ECmul
Terminal computation	5 (+2)* ECmul	5 ECmul 1 ECadd	5 ECmul 1 ECadd
Rounds of communication	9	2 (+1)**	2 (+1)**

* When using PACE with the generic mapping. ** For similar privacy protection as provided by PACE against compromised, but still authorized terminals.

4.3 Implementation Considerations

While all protocols can be run on the hardware as provided by the chips in current ePassports, one must also take into account the overhead for a secure implementation. The resulting chip implementation should be able to resist side-channel and fault injections attacks. In general, SIGMA-I and IBIHOP+ are better protected against these attacks because the adversary cannot send arbitrary messages to the chip. For the combination of PACE and EAC, an adversary with access to the ePassport can always successfully perform PACE. In chip authentication that follows after PACE, the adversary can provide any value (as long as it is a valid point on the curve) to which the chip will apply its secret by elliptic curve multiplication. Furthermore, for the proposed authentication protocols, the chip will only apply its secret to the value that is coming from a genuine and authorized terminal in the scalar domain, which is easier to protect against information leakage.

As an additional benefit the descriptions of the both SIGMA-I and IBIHOP+ are less complex (fewer rounds of communication, no need to restart secure communication ...), allowing for a clearer security and privacy assessment and leaving less room for implementation errors.

5 Conclusion

In this paper we proposed an alternative for the current combination of PACE and EAC, needed to authenticate European ePassports and read out all data. For our alternative, we proposed two possible authentication protocols that can both run on the hardware as provided by current ePassports. We showed that for each of these protocols, the proposed alternative achieves better security and privacy properties, while also improving the performance. This means that now during ePassport authentication more time can be spent on thoroughly verifying the biometrics stored within the ePassport.

From the two protocols, our new protocol IBIHOP+ is the clear winner, requiring only three elliptic curve multiplications on the tag side and two rounds of communication. By using IBIHOP+ instead of the current combination PACE + EAC, when abstracting away from the time needed for the ePassport to verify the terminal's certificate, a speed-up of at least 40% is expected for the mutual authentication procedure between the chip and terminal.

Acknowledgements

This work was supported by the European Commission through the FIDELITY EU-FP7 project (Grant No. SEC-2011-284862) and the Research Council KU Leuven: GOA TENSE (GOA/11/007).

References

[AKQ08] Gildas Avoine, Kassem Kalach, and Jean-Jacques Quisquater. ePassport: Securing International Contacts with Contactless Chips. In *Financial Cryptography and Data Security*, volume 5143 of *Lecture Notes in Computer Science*, pages 141–155. Springer, 2008.

[BFK09] Jens Bender, Marc Fischlin, and Dennis Kügler. Security Analysis of the PACE Key-Agreement Protocol. In *Information Security*, volume 5735 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 2009.

[BFK13] Jens Bender, Marc Fischlin, and Dennis Kügler. The PACE—CA Protocol for Machine Readable Travel Documents. In *Trusted Systems*, volume 8292 of *Lecture Notes in Computer Science*, pages 17–35. Springer, 2013.

[BN00] Mihir Bellare and Chanathip Namprempre. Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. In *Advances in Cryptology – ASIACRYPT 2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 531–545. Springer, 2000.

[BPBP13] Nicolas Buchmann, Roel Peeters, Harald Baier, and Andreas Pashalidis. Security Considerations on Extending PACE to a Biometric-Based Connection Establishment. In *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*, Lecture Notes in Informatics (LNI), pages 15–26, Darmstadt,DE, 2013. Bonner K´ollen Verlag.

[BSI10] BSI. *Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI).* Bundesamt für Sicherheit in der Informationstechnik (BSI), 2.05 edition, 2010.

[CLRPS07] Dario Carluccio, Kerstin Lemke-Rust, Christof Paar, and Ahmad-Reza Sadeghi. E-Passport: The Global Traceability Or How to Feel Like a UPS Package. In *Information Security Applications*, volume 4298 of *Lecture Notes in Computer Science*, pages 391–404. Springer, 2007.

[HHJ+08] Jaap-Henk Hoepman, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk, and Ronny Wichers Schreur. Crossing Borders: Security and Privacy Issues of the European e-Passport. *CoRR*, abs/0801.3930, 2008.

[HPP14] Jens Hermans, Roel Peeters, and Bart Preneel. Proper RFID Privacy: Model and Protocols. *IEEE Transactions on Mobile Computing*, 99(PrePrints):14 pages, 2014.

[HPVP11] Jens Hermans, Andreas Pashalidis, Frederik Vercauteren, and Bart Preneel. A New RFID Privacy Model. In Vijay Atluri and Claudia Diaz, editors, *2011st European Symposium on Research in Computer Security (ESORICS 2011)*, volume 6879 of *Lecture Notes in Computer Science*, pages 568–587. Springer-Verlag, 2011.

[ICA06] ICAO. *Doc 9303 Part 1 Machine Readable Passports Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capability.* International Civil Aviation Organization (ICAO), 6 edition, 2006.

[ICA13] ICAO. *SUPPLEMENT to Doc 9303*. International Civil Aviation Organization (ICAO), 12 edition, 2013.

[Kra03] Hugo Krawczyk. SIGMA: The 'SIGn-and-MAc' Approach to Authenticated Diffie-Hellman and Its Use in the IKE-Protocols. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 400–425. Springer, 2003.

[PHF13] Roel Peeters, Jens Hermans, and Junfeng Fan. IBIHOP: Proper Privacy Preserving Mutual RFID Authentication. In *Workshop on RFID and IoT Security - RFIDSec Asia 2013*, Cryptology and Information Security, pages 45–56, Guangzhou,China, 2013. IOS PRESS.

[Sch91] Claus-Peter Schnorr. Efficient Signature Generation by Smart Cards. *J. Cryptology*, 4(3):161–174, 1991.