Chip Authentication for E-Passports: PACE with Chip Authentication Mapping v2

Lucjan Hanzlik, Mirosław Kutyłowski

Wrocław University of Science and Technology, Poland

ISC 2016, Honolulu

Electronic Passport

e-passport and ebooth:

1. automatic travel document inspection
2. high security level
3. an advanced cryptographic scheme behind it

E-Passport
general data

hardware

- a chip embedded into a travel document,
- wireless communication with a reader

E-Passport
general data

hardware

- a chip embedded into a travel document,
- wireless communication with a reader

passive EPassport functions

electronic copy of the holder's data,
in particular: biometry (high quality face image, fingerprints)

E-Passport
general data

hardware

- a chip embedded into a travel document,
- wireless communication with a reader

passive EPassport functions

electronic copy of the holder's data,
in particular: biometry (high quality face image, fingerprints)

active functions

a secure cryptographic suite for interaction with a Document Verifier

Security issues

data quality

passport holder's data confirmed by the passport Issuer in a strong cryptographic way:

upside: data forgery infeasible (as long as crypto not broken)

downside: high quality data might be transferred to a third party
$\Rightarrow$ a digital signature for personal data authentication **creates a security threat**

Security issues

data quality

passport holder's data confirmed by the passport Issuer in a strong cryptographic way:

upside: data forgery infeasible (as long as crypto not broken)

downside: high quality data might be transferred to a third party
$\Rightarrow$ a digital signature for personal data authentication **creates a security threat**

ePassport as a "ticket"

no clones: infeasible to create a device mimicking the ePassport, e.g. no *replay attacks*

presence: the ePassport must be physically present during inspection

Security issues

data quality

passport holder's data confirmed by the passport Issuer in a strong cryptographic way:

- upside: data forgery infeasible (as long as crypto not broken)
- downside: high quality data might be transferred to a third party
  $\Rightarrow$ a digital signature for personal data authentication **creates a security threat**

ePassport as a "ticket"

- no clones: infeasible to create a device mimicking the ePassport, e.g. no *replay attacks*
- presence: the ePassport must be physically present during inspection

unauthorized use

ePassport must not be activated without the consent of its holder

Requirements
for ePassport

The verifier must be sure that:

1. he is talking with a genuine ePassport
2. the data received really come from this ePassport

The ePassport:

1. must know that it is talking with an authorized reader
2. interacts only when presented by its holder

In particular, ePassport must be a secure device, working exactly according to specification and manipulation resistant.

ICAO standards
International Civil Aviation Organization

Role of ICAO

- ICAO creates the facto standards
- if a passport has to be recognized worldwide, then it necessary to adhere to the standard
- pragmatic: minimalistic requirements, somewhat insecure
- ... but improving step by step

Problems

1. 10 years validity period for passports, backward compatibility
2. conflicting interests/approaches (e.g. regarding personal data protection)
3. system scale, number of authorities worldwide making final decisions

Design criteria

hardware

- simple and inexpensive chip
- small memory, low computational complexity, low communication complexity

protocols

- long term stability of protocols
- future security extensions without major rebuilding

system

- minimalistic infrastructure
- standard components, solutions already checked in practice, ...

Basic Components

Terminal Authentication

the terminal proves its rights to access the data from the ePassport

Chip Authentication

the ePassport proves that it is a genuine one and has been issued by the passport authorities

Password Authentication

the ePassport checks that the reader has got a password/Card Access Number/PIN from the document holder

Secure Channel

a channel established between the reader and the ePassport guarantees data confidentiality and integrity

Realization

Optimization

- try to achieve combined goals with one protocol
- time and space complexity is critical – strict bounds
- hardware acceleration for certain cryptographic operations
  –no freedom to redesign the cryptographic coprocessor

PACE
main points

Password Authenticated Connection Establishment

1. creates an authenticated encrypted channel iff correct password used by the reader
2. password guessing as hard as possible:
   - a reader interacting with a chip may try one password per session
   - no offline dictionary attacks
3. designed by German BSI authority, adopted by ICAO
4. in the future obligatory for biometric passports in the EU

PACE
versions

PACE-GM

PACE General Mapping: originally designed by BSI designed to avoid US patents

PACE-IM

PACE Integrated Mapping: PACE redesigned in France simplifications, efficiency improvements

(again patents)

PACE-GM
parameters

Chip	Reader
holds: π - password parameters	holds: π - password, input from owner

PACE
password dependent data

Chip		Reader
$K_\pi := H(0\|\|\pi)$		$K_\pi := H(0\|\|\pi)$
choose $s \leftarrow \mathbb{Z}_q$		
$z := ENC(K_\pi, s)$		
	$\xrightarrow{z}$	
		$s := DEC(K_\pi, z)$
choose $y_A \leftarrow \mathbb{Z}_q^*$		choose $y_B \leftarrow \mathbb{Z}_q^*$
$Y_A := g^{y_A}$		$Y_B := g^{y_B}$
	$\xleftarrow{Y_B}$	
	$\xrightarrow{Y_A}$	
abort if $Y_B \notin \langle g \rangle \backslash \{1\}$		abort if $Y_A \notin \langle g \rangle \backslash \{1\}$
$h := Y_B^{y_A}$, $\hat{g} := h \cdot g^s$		$h := Y_A^{y_B}$, $\hat{g} := h \cdot g^s$
choose $y'_A \leftarrow \mathbb{Z}_q^*$		choose $y'_B \leftarrow \mathbb{Z}_q^*$
$Y'_A := \hat{g}^{y'_A}$		$Y'_B := \hat{g}^{y'_B}$
	$\xleftarrow{Y'_B}$	
	$\xrightarrow{Y'_A}$	
check $Y'_B \neq Y_B$		check $Y'_A \neq Y_A$
$K := Y'^{y'_A}_B$		$K := Y'^{y'_B}_A$
$K_{...} := H(...\|\|K)$		$K_{...} := H(...\|\|K)$

PACE

the first DH key exchange - base establishment

Chip		Reader
$K_\pi := H(0\|\|\pi)$		$K_\pi := H(0\|\|\pi)$
choose $s \leftarrow \mathbb{Z}_q$		
$z := ENC(K_\pi, s)$		
	$\xrightarrow{z}$	
		$s := DEC(K_\pi, z)$
choose $y_A \leftarrow \mathbb{Z}_q^*$		choose $y_B \leftarrow \mathbb{Z}_q^*$
$Y_A := g^{y_A}$		$Y_B := g^{y_B}$
	$\xleftarrow{Y_B}$	
abort if $Y_B \notin \langle g \rangle \backslash \{1\}$	$\xrightarrow{Y_A}$	abort if $Y_A \notin \langle g \rangle \backslash \{1\}$
$h := Y_B^{y_A}$, $\hat{g} := h \cdot g^s$		$h := Y_A^{y_B}$, $\hat{g} := h \cdot g^s$
choose $y'_A \leftarrow \mathbb{Z}_q^*$		choose $y'_B \leftarrow \mathbb{Z}_q^*$
$Y'_A := \hat{g}^{y'_A}$		$Y'_B := \hat{g}^{y'_B}$
	$\xleftarrow{Y'_B}$	
	$\xrightarrow{Y'_A}$	
check $Y'_B \neq Y_B$		check $Y'_A \neq Y_A$
$K := Y'^{y_A}_B$		$K := Y'^{y_B}_A$
$K_{\ldots} := H(\ldots\|\|K)$		$K_{\ldots} := H(\ldots\|\|K)$

PACE

the second Diffie-Hellman for key establishment

Chip		Reader
$K_\pi := H(0\|\|\pi)$		$K_\pi := H(0\|\|\pi)$
choose $s \leftarrow \mathbb{Z}_q$		
$z := ENC(K_\pi, s)$		
	$\xrightarrow{z}$	
		$s := DEC(K_\pi, z)$
choose $y_A \leftarrow \mathbb{Z}_q^*$		choose $y_B \leftarrow \mathbb{Z}_q^*$
$Y_A := g^{y_A}$		$Y_B := g^{y_B}$
	$\xleftarrow{Y_B}$	
	$\xrightarrow{Y_A}$	
abort if $Y_B \notin \langle g \rangle \backslash \{1\}$		abort if $Y_A \notin \langle g \rangle \backslash \{1\}$
$h := Y_B^{y_A}$, $\hat{g} := h \cdot g^s$		$h := Y_A^{y_B}$, $\hat{g} := h \cdot g^s$
choose $y'_A \leftarrow \mathbb{Z}_q^*$		choose $y'_B \leftarrow \mathbb{Z}_q^*$
$Y'_A := \hat{g}^{y'_A}$		$Y'_B := \hat{g}^{y'_B}$
	$\xleftarrow{Y'_B}$	
	$\xrightarrow{Y'_A}$	
check $Y'_B \neq Y_B$		check $Y'_A \neq Y_A$
$K := {Y'_B}^{y'_A}$		$K := {Y'_A}^{y'_B}$
$K_{...} := H(...\|\|K)$		$K_{...} := H(...\|\|K)$

PACE

final phase - proof of possession and deriving keys

Chip		Reader
...		...
$K := Y'_B{}^{y_A}$		$K := Y'_A{}^{y_B}$
$K_{ENC} := H(1\|\|K)$		$K_{ENC} := H(1\|\|K)$
$K_{MAC} := H(2\|\|K)$		$K_{MAC} := H(2\|\|K)$
$K'_{MAC} := H(3\|\|K)$		$K'_{MAC} := H(3\|\|K)$
$T_A :=$ $MAC(K'_{MAC}, (Y'_B, \mathcal{G}))$		$T_B :=$ $MAC(K'_{MAC}, (Y'_A, \mathcal{G}))$
	$\xleftarrow{T_B}$	
abort if T_B invalid		
	$\xrightarrow{T_A}$	
		abort if T_A invalid

- the chip interrupts if it discovers that the tag of the reader is wrong,
- until this moment **all data sent to the reader by the chip have uniform probability distribution for every password** ...
- ... and for **every choice of the reader**

PACE IM
Integrated mapping

PACE-GM

ePassport:		Reader:
choose $y_C \leftarrow_R \mathbb{Z}_q^*$		choose $y_R \leftarrow_R \mathbb{Z}_q^*$
$Y_C = g^{y_C}$		$Y_R = g^{y_R}$
	$\xleftarrow{Y_R}$	
	$\xrightarrow{Y_C}$	
abort if ...		abort if ...
$h = Y_R^{y_C}$		$h = Y_C^{y_R}$
$\hat{g} = h \cdot g^s$		$\hat{g} = h \cdot g^s$

PACE-IM

ePassport:		Reader:
		choose $r \leftarrow_R \mathbb{Z}_q^*$
	$\xleftarrow{r}$	
$\hat{g} = \mathrm{Hash}_{EC}(s, r)$		$\hat{g} = \mathrm{Hash}_{EC}(s, r)$

PACE CAM

password authentication, key establishment, chip authentication

Goal

make minimal changes in PACE so that it provides chip authentication as well

History

- reusing randomness for Schnorr Signature:

  PACE-AA Protocol for Machine Readable Travel Document, and its Security, J.Bender, Ö.Dagdelen, M. Fischlin, D.Kügler, Financial Crypto 2012

- the current trick from CAM:

  Simplified PACE-AA Protocol, L.Hanzlik, L.Krzywiecki, M.Kutyłowski, ISPEC 2013, May 2013

- the same:

  The PACE-CA Protocol for Machine Readable Travel Documents, J.Bender, M. Fischlin, D.Kügler, INTRUST 2013, 2013

- adopted by ICAO under the name CAM:

  ISO/IEC JTC1 SC17 WG3/TF5 for ICAO. Supplemental Access Control for Machine Readable Travel Documents v1.1. April 2014.

PACE CAM
Slides from ISPEC'2013

Chip		Reader
π x_A, $X_A = g^{x_A}$		π
random s chosen	$\xrightarrow{ENC(K_\pi, s)}$	retrieve s
choose $y_A \leftarrow \mathbb{Z}_q^*$		choose $y_B \leftarrow \mathbb{Z}_q^*$
$Y_A := g^{y_A}$		$Y_B := g^{y_B}$
abort if ...	$\xrightarrow{Y_A}$	abort if ...
$h := Y_B^{y_A}$, $\hat{g} := h \cdot g^s$		$h := Y_A^{y_B}$, $\hat{g} := h \cdot g^s$
choose $y'_A \leftarrow \mathbb{Z}_q^*$		choose $y'_B \leftarrow \mathbb{Z}_q^*$
$Y'_A := \hat{g}^{y'_A}$	$\xleftarrow{Y'_B}$	$Y'_B := \hat{g}^{y'_B}$
check ...	$\xrightarrow{Y'_A}$	check ...
$K_{...} := H(...\|\|{Y'_B}^{y'_A})$		$K_{...} := H(...\|\|{Y'_A}^{y'_B})$
...tags checked	...	...tags checked
	$\xrightarrow{E_{K'_{SC}}(w, cert_A))}$	
$w := y_A / x_A$		decrypt with K'_{SC}
		check certificate $cert_A$
		abort if $X_A^w \neq Y_A$

PACE CAM, more secure version (not adopted by ICAO)

Slides from ISPEC'2013

Chip		Reader
π, x_A, $X_A = g^{x_A}$		π
random s chosen	$\xrightarrow{ENC(K_\pi, s)}$	retrieve s
choose $y_A \leftarrow \mathbb{Z}_q^*$		choose $y_B \leftarrow \mathbb{Z}_q^*$ $Y_B := g^{y_B}$
$Y_A := X_A^{y_A}$		
	$\xleftarrow{Y_B}$	
	$\xrightarrow{Y_A}$	
abort if ...		abort if ... $h := Y_A^{y_B}$, $\hat{g} := h \cdot g^s$
$h := (Y_B^{y_A})^{x_A}$, $\hat{g} := h \cdot g^s$ choose $y'_A \leftarrow \mathbb{Z}_q^*$		choose $y'_B \leftarrow \mathbb{Z}_q^*$
$Y'_A := \hat{g}^{y'_A}$	$\xleftarrow{Y'_B}$	$Y'_B := \hat{g}^{y'_B}$
	$\xrightarrow{Y'_A}$	
check ... $K_{...} := H(...\|\|Y'^{y'_A}_B)$ ...tags checked	...	check ... $K_{...} := H(...\|\|Y'^{y'_B}_A)$ ...tags checked
	$\xrightarrow{E_{K'_{SC}}(w, cert_A))}$	
$w := y_A$		decrypt with K'_{SC} check certificate $cert_A$ abort if $X_A^w \neq Y_A$

PACE CAM versus IM

Problems

- it does work for PACE GM only
- but PACE IM more efficient

should we fall back to PACE GM?

- No. Solution given in this paper
- Moreover, the security argument based on reduction to a standard crypto assumption (SDH-2).

PACE CAM with PACE IM

new version for the SAC standard

ePassport:		Reader:
password π		password π
secret key sk_C		
public key pk_C		
certificate $cert_C$ for pk_C		
$K_\pi = \mathrm{Hash}(\pi)$		$K_\pi = \mathrm{Hash}(\pi)$
choose $s \leftarrow \mathbb{Z}_q$		
$z = \mathrm{Enc}(K_\pi, s)$	$\xrightarrow{z}$	
		$s = \mathrm{Dec}(K_\pi, z)$
	Mapping Function	
derive $\hat{g_1}$ with IM or GM		derive $\hat{g_1}$ with IM or GM
choose $y'_C \leftarrow \mathbb{Z}_q^*$		choose $y'_R \leftarrow \mathbb{Z}_q^*$
$Y'_C = \hat{g_1}^{y'_C}$		$Y'_R = \hat{g_1}^{y'_R}$
	$\xleftarrow{Y'_R}$	
	$\xrightarrow{Y'_C}$	
$K = {Y'_R}^{y'_C}$		$K = {Y'_C}^{y'_R}$
derive other keys from K		derive other keys from K
$w = y'_C / sk_C$		
$c = \mathrm{Enc}(K'_{\mathrm{Enc}}, (w, cert_C))$		
	$\xrightarrow{c}$	
		$(w, cert_C) = \mathrm{Dec}(K'_{\mathrm{Enc}}, c)$
		check $cert_C$ and extract pk_C
		abort if $e(Y'_C, g_2) \neq e(\hat{g}, pk_C)^w$

PACE CAM with IM
properties

implementation issues

- pairings used, but only on the side of the reader
- the ePassport needs to perform computations in the first group only
- computing pairings on the reader is not a problem (no resource limitations)

Main properties
properties

AKE Security

easy, follows from the proof for PACE

Impersonation Resistance

a draft to be in the paper: a reduction to 2-Strong DH Problem:

$$\textit{Given } (g_1, g_1^x, g_1^{x^2}, g_2, g_2^x) \in \mathbb{G}_1^3 \times \in \mathbb{G}_2^2,$$
$$\textit{output } (c, g_1^{1/(x+c)}) \in \mathbb{Z}_q \times \mathbb{G}_1.$$

the reduction construction is relatively short, but tedious to follow

Other

other nice properties inherited from PACE: simultability, behavior during faulty sessions, resilience to ephemeral key leakage, ...
proofs analogous to the ideas from ISPEC 2013

Conclusions

Achieved

- security based on a standard assumption
- no pairings on the chip required
- minimal changes to the existing standard

Challenges

- is it optimal?
  hard to imagine how to simplify it...
- it might be that we still have no ultimate solution for all ePassport components (e.g. Terminal Authentication and its PKI)

Thanks for your attention!

Contact data

1. Miroslaw.Kutylowski@pwr.edu.pl
2. http://kutylowski.im.pwr.edu.pl
3. http://cs.pwr.edu.pl