Homework 1

Encryption

Botond Lajos Perényi

1 System Requirements

1. **The system must manage encryption keys and signing keys securely, including usage of Hardware Security Modules (HSMs) where applicable**
   Dedicated HSMs is not guaranteed in mobile devices, but the cloud can be built with such modules. However, the paper does not describe any specifics about this issue.

2. **The e-ID data must be encrypted using strong, industry-standard encryption algorithms**
   The usage of LUOV scheme is unsafe. It is based on UOV, which has been proved to be insecure by multiple papers. [BWP04] [FP09] The improvements were introduced to make the LUOV useful in the post quantum stage, but they are also proven to be insecure with most usual parametrizations. [Din+19]

3. **The system should rely on use of digital signatures to verify the authenticity of the e-ID data and to ensure that the data has not been tampered with**
   In the issuing protocol there is no mechanism for signing the request. In the presentation protocol, the PR sends its ID with a signature, and checks the receiving request with decrypting and checking if the resulting plaintext is "meaningful". However, meaningful data is not guaranteed with many personal data, such as names, addresses, etc.

4. **The system must ensure that e-ID that was not created by the issuer does not pass verification by the RP**
   This does not hold. There is no check specified in the documentation for the RP to filter out, at any point requests, that are not authenticated by the issuer. One can create an e-ID, and send it to RP without communicating with the issuing party, and this request would be validated, and then the forger would be authenticated as an honest user.

5. **The system must ensure post-quantum security for all the components**
   The paper lists different encryption and signature schemes, which it recommends to use, but only two of the presented are considered post-quantum: SHA3 and LUOV. Moreover, the presentation protocol uses ECDSA, which is not considered suitable for post-quantum (as it uses a discrete logarithm problem, which can be broken with a quantum-computer).

6. **The system must use standardised cryptographic algorithms**
   This requirement is met. The paper does not introduce new cryptographic algorithms, which is laudable. However some of the described standardised cryptographic algorithms are outdated, or advised against. (Specifically DES [Nat05])

7. **The system must ensure that attackers getting access to the user's device are not able present honest user's credential to the RP**
   There is no mechanism specified in the document, that can ensure this requirement. It is easy to create a PIN-locked application for this purpose, but there is no mention at all in the paper on this.

8. **The system must ensure strong user authentication before credential is issued**
   The specification calls for verification by photo, which can be considered secure. [Pra+20] However a photo is easily accessible (from e.g Facebook), which makes the scheme vulnerable to attacks.

9. **The system must ensure that adversary cloning the mobile device memory, does not gain access to user' private information**
   This is not explicitly addressed in the paper, but it is suggested that the mobile device stores personal data in either encrypted (better), or unencrypted (much worse) form. It would be better if a hash of the personal data would be stored instead of and encrypted form. (A hash cannot be broken, only collisions can be explored.)

10. **The system must ensure that adversary cloning the mobile device memory is not able to issue revocation, issuing and presentation requests (without active participation of user)**
    This is not satisfied, as the paper states, that the device stores the `uid` and the photo, that was used to the issuing and presentation request.

* The paper advises against TLS on the grounds of efficiency. I would be vary of this, because TLS is established to be secure, and the newest version (1.3) is pretty efficient. (Only 1500-4500 bytes per handshake, which is not a significant amount using current day technology, especially compared to sending a photo.) [Res18]

2 Additional inconsistencies and other problems

The revocation protocol calls for a method, in which the issuing party can revoke an ID, but it does not have a description of such scheme.
Also, the revocation protocol needs the application in the hands of the user, which might not be true, especially after the mobile device has been stolen. For this case there is a need for another way of revoking an e-ID.
Storing the e-ID securely by uploading to the "cloud" is not impossible, but there is no specification on what kind of security mechanism (encryption) would be used, and how would this make the scheme secure.
The paper calls the system convenient, but I would argue, that changing an e-ID each time a personal detail changes, such as address, would work against convenience. It would be better to base the verification on things, that are never expected to change (e.g.: birth date, name at birth, mother's maiden name).

3 Final conclusion

The paper is sometimes vague, and leaves a lot for individual interpretation and implementation. Thus implementing it would not satisfy basic security expectations, that are raised in the paper.
There are a lot of goals described in the paper, but some are not met, or they are left for the implementation to deal with.

References

[BWP04] An Braeken, Christopher Wolf, and Bart Preneel. *A Study of the Security of Unbalanced Oil and Vinegar Signature Schemes*. Cryptology ePrint Archive, Paper 2004/222. 2004. URL: https://eprint.iacr.org/2004/222.

[Nat05] National Institute of Standards and Technology. *Announcing Approval of the Withdrawal of Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation*. https://www.govinfo.gov/content/pkg/FR-2005-05-19/pdf/05-9945.pdf. Federal Register, Vol. 70, No. 96, pp. 28907–28908. May 2005.

[FP09] Jean-Charles Faugère and Ludovic Perret. *On the Security of UOV*. Cryptology ePrint Archive, Paper 2009/483. 2009. URL: https://eprint.iacr.org/2009/483.

[Res18] Eric Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. Section 4.1.2. Internet Engineering Task Force, Aug. 2018. DOI: 10.17487/RFC8446. URL: https://www.rfc-editor.org/rfc/rfc8446.html.

[Din+19] Jintai Ding et al. "New Attacks on Lifted Unbalanced Oil Vinegar". In: *Second NIST Post-Quantum Cryptography Standardization Conference*. Santa Barbara, CA, USA, Aug. 2019. URL: https://csrc.nist.gov/CSRC/media/Events/Second-PQC-Standardization-Conference/documents/accepted-papers/ding-new-attacks-luov.pdf.

[Pra+20] D. Praveenbalaji et al. "ID Photo Verification by Face Recognition". In: *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*. 2020, pp. 1449–1453. DOI: 10.1109/ICACCS48705.2020.9074246.