Dr. Jordi Castellà-Roca
Head of Department
Associate professor
Departament d'Enginyeria Informàtica i Matemàtiques
UNESCO Chair in Data Privacy
Centre de recerca en ciberseguretat de Catalunya (CYBERCAT)
Universitat Rovira i Virgili
Av. Països Catalans, 26
E-43007 Tarragona (Catalonia) - Spain
Tel. +34 977558876 Fax. +34977559710
Email: jordi.castella@urv.cat

August 9th, 2019

Summary of the thesis

It's difficult to imagine all possibilities that a connected world (Internet of Things - IoT) will offer us, but it's easy to predict that the security has to be mandatory. We must be sure that connections have been established directly between the expected devices. Therefore, the current thesis tackles this important topic, i.e. the secure authentication. However, it does taking into account the following requirements: privacy, efficiency and real deployment. Regarding the privacy, the contributions meet the following privacy properties: i) anonymity; ii) unlinkability; iii) untraceability and; iv) revocation of anonymity. The fulfillment of the first three properties assures a strong privacy, while the last one allows to identify users in case of bad behavior.

The efficiency, or improvement of the previous authentication protocols, is important because the devices used in IoT have computation, communication and memory limitations. Finally, it's making positive the concerns about the feasibility to deploy the proposals. They are not merely theoretical.

The thesis is organized in the following parts: i) background; ii) state of the art; iii) multi-device authentication scheme where the user proves that she takes with her (wears) multiple devices (safety equipment); iv) cryptographic scheme based on group signatures for smart metering systems; v) elliptic curve variant of the HM12 Attribute-Based credential scheme that improves its performance and; vi) keyed-verification anonymous credentials that improves the performance against previous proposals and it includes an analysis of all major programmable smart card platforms.

The background contains the notation used in the thesis and the computational hardness assumptions on which are based some of the proposals (integer factorization, RSA, Strong RSA, DL, CDH, SDH, DDH, SDDH and SDDHI). Next, there is an introduction to the Elliptic Curve Cryptography (ECC): i) definition; ii) operations; iii) elliptic curve forms and; i) bilinear pairing. The section also includes an explanation of the concept of proof of knowledge. It's widely used in the protocols of the thesis. Moreover, there is a description of the Weak Boneh-Boyen signature and the Okamoto-Uchiyama Encryption. Finally, the concept of Algebraic Message Authentication Code (MAC) is introduced. The background is fairly comprehensive and particularly useful.

The state of the art is divided into three sections: i) group signatures; ii) attribute-based credentials and; iii) smartcards. The group signatures section introduces the entities involved (users, verifiers, group manager and revocation manager), the security properties (authenticity, integrity, completeness, soundness and unforgeability, revocation, differentiation of group members), the privacy properties (anonymity, unlinkability, coalition resistance, framing resistance, traceability and unforgeable traeability), and practical properties (dynamism and efficiency). There is an interesting comparison of the main proposals of group signatures schemes (BBS, DP, HLCCN, ACJT, CG, IMSTY and HMGS), more precisely the following items are evaluated for each scheme: i) signature cost; ii) verification cost; iii) signature size; iv) public key size; v) allow pairing; vi) computational hardness assumptions and; vii) revocation. The schemes have been implemented allowing to obtain the performance (time). The attribute-based credentials section describes the actors involved (users, issuers, verifiers and manager), the security properties (authenticity, integrity, confidentiality, non-transferability and revocability) and privacy properties (anonymity, unlinkability, untraceability and selective disclosure of attributes). Next, the following schemes are explained in more detail and implemented in order to compare them: i) U-Prove; ii) Idemix and; iii) HM12 (Hajny-Malina). The smartcards section briefly introduces the smartcard categories (memory and microprocessor cards), the application programming interface and, the main smartcard platforms (Java Card, MultOs, Basic Card, .NET Card). There is an interesting study about the cryptographic and mathematical support of the aforementioned platforms, and a performance comparison.

The multi-device authentication scheme is the alleged first contribution. Although, the previous implementations and studies of group signatures, attribute-based credentials and smartcards could be considered really the first contribution.

The proposal is focused on safety applications in which the users have to wear multiple safety components (helmet, boots, protections, etc…). The authentication is possible when the user wears all the equipment (components). The authentication preserves the users' privacy (anonymity, unlinkability, untraceability and, revocation). There are four operations (setup, keygen, register and authenticate). The scheme uses the wBB signature to certify the identifiers of the components (tags) in the register phase, and interactive proofs of knowledge to prove the knowledge of respective signatures and identifies in the authentication. The protocol performance has been evaluated using a smartcards (MultOS), a smartphone (HUAWEI P9 Lite 2019) and a smartwatch (HUAWEI Watch 2) as the user's components (tags). The proofs can be generated under 500 ms, but the verification time grows linearly with the number of components (tags) involved in the authentication protocol.

The anonymous data collection scheme is suitable for an energy supplier (collector) who performs statistical evaluations on the consumption in a given area. The collector can be assured that data are collected from trusted sources and were not modified during a transfer. It's assumed that smart metering devices are constrained devices with very limited computational power and memory. The scheme has the following operations: i) setup; ii) register; iii) sign; iv) verify and; v) revoke. The user (smart metering device) obtains a wBB signature on its private identifier from the manager. Next, the device proves the knowledge of such a signature anonymously using the Schnorr-like zero-knowledge protocol by means of the knowledge of a discrete logarithm. The scheme has been implemented in order to evaluate its performance. The signing times ranges from 362 ms (smartcard) to 2.889 ms (Watch).

The anonymous credential with practical revocation contribution is a variant of the HM12 attribute-based credential scheme. It has been modified in order to use elliptic curves obtaining an improvement (computing time and communication transfer) compared with the initial proposal. The scheme has the following operations: i) setup; ii) issue attributes (it's divided in two parts); iii) prove attributes and; iv) revoke. As with the previous schemes, the scheme has been implemented (MultOS ML4 smart card) in order to compare it with the initial proposal. The prove attributes operation is about 20% faster than in the initial proposal and a 40% faster considering the communication overhead. However, the revocation process is linear in relation to the number of users while the initial proposal is constant.

The last contribution is a keyed-verification anonymous credential scheme. The scheme has been designed taking into account that implementations have to use smartcards. Moreover, there is an analysis of all major programmable smartcard platforms regarding the availability and performance of EC operations.

The scheme actors are the users, the issuer and the verifier. However, the issuer and the verifier are the same entity. The verifier needs the issuer's secret keys in order to verify the users' attributes. This allows to omit some elements that the verifier can compute by itself saving work to the prover. The scheme has the following operations: i) setup (it includes the setup of the group and the credential key generation); ii) issue attributes (it includes the issue of the credentials and obtaining/verifying the Credentials) and; iii) prove attributes. The prove operation is based on demonstrate knowledge of a weak Boneh-Boyen signature applying the proofs due to Arfoui et al. and Camenisch et al. The scheme efficiency is studied by means of the comparison of the exponentiations required (or scalar multiplications of EC points), the fulfillment of the unlinkability property, use of a MAC, and security assumptions. The scheme is compared with U-Prove, Idemix, Ringers et al., MAC M. Chase et al. and, A. Barki et al. The proposal is the most efficient among those that fulfill the unlinkability propery. The implementation and performance analysis contains two parts: i) smartcard selection and; ii) implementation results. The following smartcards have been included in the study: J3A081, J3D081, SmartCafe6, SmartCafe5, ZC7.6, ML4 and ML3. For each smartcard the following properties has been evaluated: ECDSA, ECDH, EC addition, EC multiplication and, EC inverse. The scheme implementation has been compared (2 stored attributes, 3 stores attributes, 4 stored attributes and 5 stored attributes) with the Vullers and Alpár implementation of Idemix (the second most efficient that fulfills the unlinkability property). The proposal is at least 44% faster in all cases.

Comments

1-Is the topic appropriate to the particular area and is it up-to-date from the viewpoint of the present level of knowledge?

The thesis discusses and proposes practical solutions to protect the digital identity. Nowadays, we can assert that digital identity is a central and key issue, given the deployment of the Industry 4.0 (Cyber-Physical Systems, Internet of Things, Industrial Internet of Things, Cloud Computing, Cognitive Computing and Artificial Intelligence). The interaction between users, devices, systems, etc.. in the new paradigm has to be secure and therefore the first step is the authentication. Furthermore, the proposals include "by design" the following properties: i) privacy; ii) performance and; iii) practical deployment. The state-of-the-art is up-to-date, but what is even more important, the proposals have been implemented using actual devices (smartcards, smart watches, smart-phones). This provides clear measure of the proposals feasibility and deployability.
The results obtained in the thesis are suitable to address the challenges that bring us the IoT.

2-Is the thesis pertinent and does it contain original aspects? Please specify the original features.

The thesis is pertinent because it provides information and results about the performance of several elliptic curves, the performance of cryptographic libraries and, operations and performance of smartcards. The results can help to other researchers that want to implement cryptographic schemes using ECC or smartcards. Moreover, there are four original contributions: i) multi-device authentication scheme; ii) cryptographic scheme based on group signatures for smart metering systems; iii) elliptic curve variant of the HM12 Attribute-Based credential scheme and; iv) keyed-verification anonymous credentials.

I would like to highlight the following original aspects:

- Comparison of the speed of elliptic curves: Short W., Edwards, Jacobian, Jacobi q., Jacobi i. and, Hessian.
- Performance evaluation of the following libraries: Pairing Based Cryptography (PBC), Multiprecision Integer and Rational Arithmetic Cryptographic Library (MIRACL), University of Tsukuba Elliptic Curve and Pairing Library (TEPLA), Efficient LIbrary for Cryptography (RELIC) and, MCL.
- Elliptic curve cryptography support of the main smartcard platforms benchmarks of ECC operations (point addition, scalar multiplication and, point inverse), benchmarks of ECC protocols in smartcards and, benchmarks of modular arithmetic and hash functions in smartcards.
- Multi-device authentication scheme where the user proves that she takes with her (wears) multiple devices. It's a novel and interesting approach for IoT. The proofs can be generated in less than 500 ms on constrained devices;
- Cryptographic scheme based on group signatures for smart metering systems. The scheme can be used in Industry 4.0 and it's outstanding efficient;
- Elliptic curve variant of the HM12 Attribute-Based credential scheme. The proposal improves the performance of the previous proposals, and;
- Keyed-verification anonymous credentials. It improves the performance against previous proposals and it includes an analysis of all major programmable smart card platforms.

3-Was the core of the thesis published at an appropriate level? (Reprints or copies of bibliographical data should be included. In exceptional cases, confirmation of acceptance for publishing in renowned journals or presenting at significant events can be accepted.)

The results (proposals) of the thesis has been published in nine international conferences with peer-review, two journals non ISI JCR, and three journals ISI JCR. All five journals are open access. That should facilitate the dissemination and increase the number of citations. In the case of the ISI JCR journals, two of them are in the third quartile and the last one in the fourth quartile. In this regard, there is some room for improvement. I suggest to publish in the first or second quartile whenever possible.

4-Does the list of candidate's publications imply that they are persons with an outstanding research erudition?

The number of publications (fourteen) that back the contents of the thesis is a demonstration of the following points: i) they are talented and hard workers; ii) the topic and hence the results are interesting and significant for the scientific community. The post of tenure-eligible lecturer is the first of the contractual teaching posts to exist in Catalonia. For recruitment to a tenure-eligible lecturer post, candidates must be in possession of a favorable report issued by AQU Catalunya. The CV of the PhD candidate would be more than enough to ensure a favorable report.

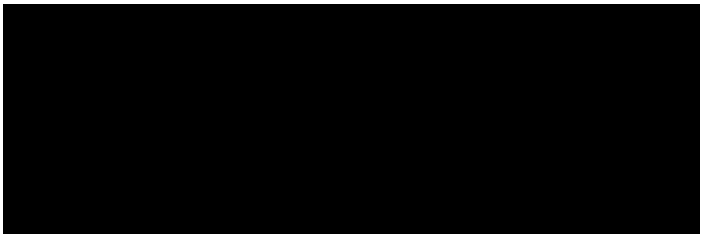
5-Some other aspects that would you characterize the personality of the candidates.

I had the pleasure of meeting the PhD candidate 4 years ago, as he was doing a research stay in the CRISES research group at the Universitat Rovira i Virgili. During his stay, I noticed that Petr was an enthusiastic, meticulous and hard-working student who did his best in order to obtain the most optimal results. He enterprisingly faces challenging problems, by proposing solutions and putting them into practice. Moreover, he applied best working methodologies and he did so really fast.

Moreover, he was ever willing to work with others in order to share his knowledge and expertise, and to learn from them also.

In conclusion, please state clearly if, in your opinion, the thesis meets the standard generally required for the awarding of an academic degree.

In my opinion the thesis amply meets the standard generally required for the awarding of an academic degree.



Dr. Jordi Castellà-Roca