COSMO
CONNECTED · SMART · MOBILITY

Technology Offer

LIS: Lightweight Signature Schemes for Continuous Message Authentication in Cyber Physical Systems

Technology Overview

Cyber-Physical Systems (CPS) provide the foundation of our critical infrastructures, which form the basis of emerging and future smart services and improve our quality of life in many areas. In such CPS, sensor data is transmitted over the network to the controller, which will make real-time control decisions according to the received sensor data. Due to the existence of spoofing attacks (more specifically to CPS, false data injection attacks), one has to protect the authenticity and integrity of the transmitted data. However, the resource constrained field devices like sensors cannot afford conventional signature computation. Thus, we introduce two Lightweight Signature schemes LiS, which are suitable for continuous message authentication commonly seen in cyber-physical systems.

Our LiS scheme has two versions, which are briefly illustrated as follows. (We refer the reader to our paper for more details). LiS1 is non-adaptively secure and suitable for small messages with a few hundred bits but is the most efficient one. The second protocol LiS2 can provide adaptive security, but one more cryptographic hash function is required.

I. Non-adaptively Secure Signature Scheme: LiS1

LiS1 relies on chameleon hash functions (CHF), Bloom filters (BF), and Universal Hash Functions (UHF). The LiS1 is briefly described as follows (see also in Figure 1).

Init: A signer A first runs the key generation algorithm of the chameleon hash function (sk ,pk) := CHF.KGen() to generate a pair of secret/public key, and samples a random key k for the universal hash function UHF, a random message M, and an initial random value r '. A initializes Bloom filter instance BF with size l and false positive parameter ε. For i∈[l], A generates l dummy random values such that r ' := UHF(k,r '), and the verify points t := CHF(M,r ') for future use. Meanwhile, A inserts those verify points into the Bloom filter BF.insert(t). A random variable r' := r ' which is used for generating the next signature. Eventually, the secret key and the verification key of A are sk := (sk , k,r',M) and vk := (BF, pk).

Sign: Upon obtaining a message m that requires authentication, the signer A first retrieves the stored secret key sk := (sk , k,r',M). A can compute the signature for m as x := CHF.Coll(sk ,r',M,m) = M* sk + r' – m* sk. Then, A can send m together with the signature x to the verifier. After this, A updates the dummy randomness to the next one as r' := UHF(k,r').

Verify: Upon receiving a message m and its signature x from the signer A, the verifier B verifies it by checking that whether the resultant hash value t=CHF(m,x) is in the Bloom filter, i.e., BF.check(t).

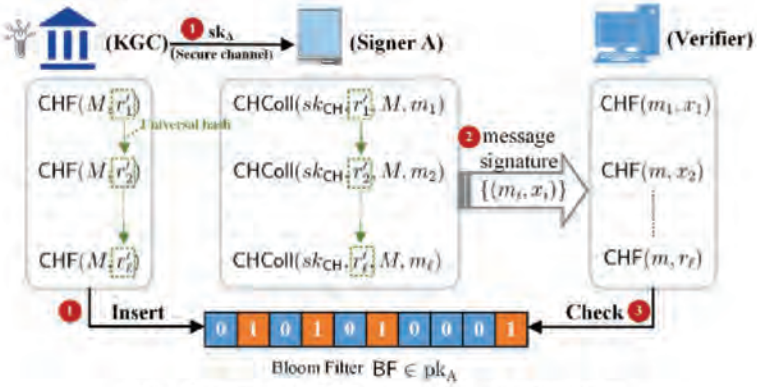

Fig. 1. Overview of LiS. KGC stands for key generation center

II. Adaptively Secure Signature Scheme: LiS2

The second version LiS2 relies on the first version scheme and a hash function H. The LiS2 is briefly described as follows.

Init: This algorithm is identical to that of LiS1.

Sign: To authenticate a message m, A first samples a random value N, and computes y := H(m||N). Then the signer A generates the signature x for y as x := CHF.Coll(sk ,r',M,y) = M* sk + r' – y* sk . Then, A can send m together with the signature x to the verifier. After this, A updates the dummy randomness to the next one as r' := UHF(k,r').

Verify: Upon receiving (m,N,x) from the signer A, the verifier B verifies it by checking that whether the resultant hash value t=CHF(H(m||N),x) is in the Bloom filter, i.e., BF.check(t).

Verification Key Replenishment. The signer can outsource the re-initialization of the new Bloom filter instance BF' to a trusted server (which is not the verifier). Then, the outsourcing server who knows the dummy randomness/message pair (r', (sk))$ and the key k of the universal hash function can compute those chameleon hash values for the signer without any interaction. The signer does not need to get involved in the verification key update, and it can keep using its signing key to sign future messages continuously. The outsourcing server (the key generation center) only needs to periodically publish a new BF' together with the server's signature to a public bulletin, which can be downloaded by the public. Nothing needs to be changed on the signer side. The system of server-aided replenishment (SAR) is depicted in Fig.2.

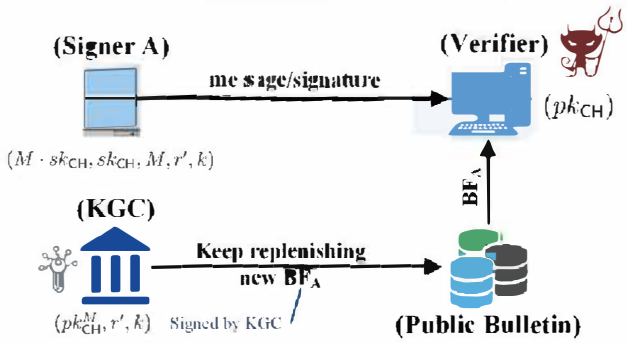

Fig. 2. Overview of Server-aided Replenishment (SAR)

Technology Features / Specifications

LiS has the following features and advantages.

1. LiS1 is strong existential unforgeable against non-adaptive chosen message attacks in the standard security model. LiS2 is strong existential unforgeable against adaptive chosen message attacks under the random oracle model. Both our DS schemes are proved without non-standard forking lemma comparing to prior Schnorr like online/offline digital signature schemes.

2. Our DS schemes enable the outsourceable verification key replenishment, in such a way that the verification key can never run out. Our replenishment has no impact on signer over prior work.

3. Due to the optimized instantiation of CHF, Our DS schemes can achieve multiple-times performance improvement over prior work.

Potential Applications

LiS1 and LiS2 can be widely used in cyber-physical systems. It enables resource-constrained signers to (continuously) authenticate messages. Below are a few examples of potential applications.

- Satellite Navigation Systems
- V2X Systems
- Maritime Systems
- Smart Grid

Benefits

The mentioned techniques provide efficient signature mechanism that can support the fast and continuous message authentication in CPS, while being easy to compute on the resource-constrained devices. Specifically, our signature schemes have a fast signing procedure and an optimal storage requirement on the signer side. The optimized signing algorithms are very efficient. Namely, our first scheme requires only three additions and two multiplications, and only one additional hash is needed in the second scheme to resist adaptive chosen message attacks. In addition, the size of the signing key in our schemes is a small constant-size bit string, which well fits CPS applications.

Please contact Prof. Zhou Jianying (SUTD) for further discussions on this technology.

Connected Smart Mobility Programme
School of Electrical and Electronic Engineering
Nanyang Technological University
50, Nanyang Avenue, S2-B3b-10, Singapore 639798
(65) 6790 5468
cosmo@ntu.edu.sg