Project Writeup

Stateful Public-Key Cryptosystems: How to Encrypt with One 160-bit Exponentiation

Zhige Xin
March 14, 2012

Motivation

The cost of computations on the discrete-exponentiation is getting serious in public key cryptography. It would be the barrier that prevents applying public key cryptography to some situation that the portable electronic devices are widely used, like cell phones. To adress this problem, this paper propose a new stateful public-key scheme that lets senders be stateful to accelerate the speed of encryption part of public-key cryptosystem. Particularly, this paper developed the traditional DHIES and Kurosawa-Desmedt schemes into stateful versions, which can be proven to meet IND-CCA security.

Stateful encryption scheme

Among the stateless, discrete-logarithm based and proven IND-CCA schemes, DHIES is most efficient because its decryption just costs 1 exponentiation. In the stateful model, the encryption of DHIES can be improved from 2 to 1 exponentiation. The new model proposed in this paper is to let senders to keep some state information, meaning that apart from the message, receiver's public-key and freshly-chosen coins, the current state and even updated state have to be computed in the process of encryption.

- Formulation: A stateful public-key encryption scheme StPE = (Setup, KG, PKCk, NwSt, Enc, Dec) contains six tuple. Each of them is an algorithm. The whole operation is shown in Figure 1. The main purpose of algorithm Setup is to produce a system parameter sp by an authority as partial input of rest algorithms. By running algorithm KG, any entity can get a public-key pk and secret key sk using input sp. The initial state of st that a sender maintains can be obtained after running algorithm NwSt. The algorithm Enc can run and output a ciphertext C for the receiver and a updated state st for the sender at any time when it gets the input sp, st and the message needed to be encrypted. And the algorithm Dec is deterministic and takes sp, sk and C as its input and returns a message M or a sign that represents an invalide ciphertext. At last, to check whether underlying group contains some components of the public-key, the algorithm PKCk is used and returns a bit 0 or 1 to show the result of the check.

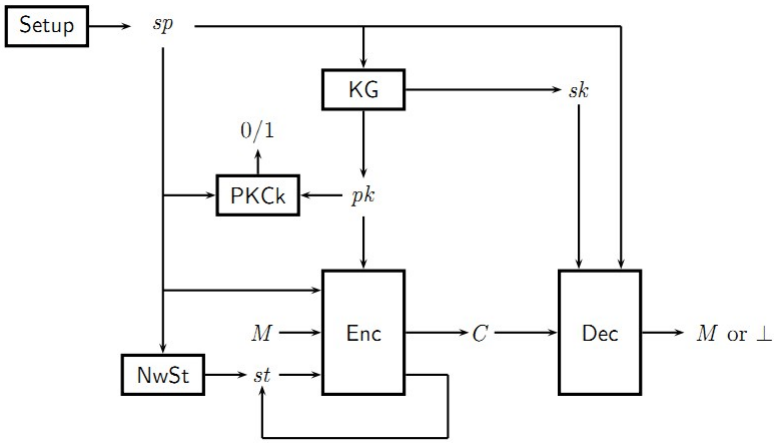

Figure 1: Stateful public-key sheme

- Basic security model: this paper used game-playing technique to define IND-CCA security of stateful public-key encryption scheme. This game starts with the initializations: sp $\xleftarrow{\$}$ Setup; $(pk_1,\ sk_1) \xleftarrow{\$}$ KG(sp); c $\xleftarrow{\$}$ 0,1; n$\leftarrow$1; st $\xleftarrow{\$}$ NwSt(sp), then adversary A can make any kinds of oracle queries if it gets sp and pk_1 and outputs a bit. Note that in the game, one sender communicates with multiple receivers, in which only one is honest and its index is 1. Four types of oracle queries exist in the game. First of all, the public keys of all other receivers is controled by A by making oracle query MKBDREC(pk), which can produce a receiver such that with its public-key, any string pk A chooses can pass the public-key verification test. In addition, via LOR(M_0,M_1), A can run ENC under the input tuple (sp, pk_1, M_c, st) to get ciphertext C. The rest oracle queries include ENCRYPT(i, M) and DECRYPT(C). A can call ENCRYPT(i, M) to obtain a ciphertext, where 1$\leq$igen and the public-key is receiver i's. If C is not returned after LOR is executed, a CCA on the honest receiver can be made via DECRYPT(C) by A. Finally, adversary A has to return a bit. Suppose the bit is d, then the IND-CCA advantage of A is as follows:

$$Adv_{StPE}^{ind-cca} = 2 \cdot Pr[d = c] - 1$$

  In this setting, USK (Unknown Secret Key) model is used. On the other hand, the only difference between using KSK (known secret key) model and USK is that MkBdRec oracle takes instead two arguments pk and sk.

The stateful DH scheme

The stateful DH scheme is a variant of DHIES such that its encryption just costs 1 exponentiation compared with 2 in the original scheme, even not increasing the decryption cost. The basic thought here is that a symmetric key is derived from g^{xr} by hash function. And then a

ciphertext and a symmetric encryption of M is sent under IND-CCA secure symmetric scheme. Of course this new model can be proven secure.

- Building blocks: The first one is through defining the gap-dh-advantage of an adversary $A_{\mathbb{G}}$ as:

$$Adv_{\mathbb{G}}^{gap-dh}(A_{\mathbb{G}}) = Pr[Z = g^{xr} : g \xleftarrow{\$} Gen(\mathbb{G}); r, x \xleftarrow{\$} \mathbb{Z}_m; Z \xleftarrow{\$} A_{\mathbb{G}}^{DDH_g(g^r,\cdot,\cdot)}(g, g^r, g^x)]$$

  where $\mathbb{G}$ is a cyclic group with m order, Gen($\mathbb{G}$) is the set of generators of $\mathbb{G}$ and the Gap-CDH problem is supposed to be hard in $\mathbb{G}$. Also, this paper gave a weaker assumption that g^r is fixed so that it suffices for the results.

  The other one is a symmetric encryption scheme SE which is assumed IND-CCA secure and its formal description is SE = (SEnc, SDec), where SEnc and SDec are its encryption and decrytion algorithm. Then the ind-cca-advantage of an adverary A_{SE}:

$$Adv_{SE}^{ind-cca}(A_{SE}) = 2 \cdot Pr[d = c : K \xleftarrow{\$} \{0,1\}^k; c \xleftarrow{\$} \{0,1\}; d \xleftarrow{\$} A_{SE}^{SEnc(K,\cdot),LOR(K,\cdot,\cdot,c),SDec(K,\cdot)}] - 1$$

- Scheme: Like the stateful scheme shown in last section, the stateful DH scheme is also composed of 6 algorithms and its formal description is: StDH = (Setup, KG, PKCk, NwSt, Enc, Dec). The Setup algorithm outputs a generator g which is randomly chosen from Gen($\mathbb{G}$) as its system parameters. KG(g) produces the secret and public keys, which are denoted by (x, X) and X respectively, where x is chosen randomly from $\mathbb{Z}_m$ and X=g^x. Whether X belongs to $\mathbb{G}$ can be checked by PKCk(g, X). NwSt(g) chooses r randomly from $\mathbb{Z}_m$ and outputs st = (r, R) where R = g^r. The encryption algorithm Enc calulates K = H(R, Z, R^x) which is k bits and symmetric ciphertext $C_s \xleftarrow{\$}$ SEnc(K, M) and eventually outputs (R, C_s) as its ciphertext and an unmodified state (r, R). If decryption algorithm is given the input g, (x, X), C = (R, C_s) and oracle H, it can returns $\perp$ if R $\notin$ $\mathbb{G}$ and returns SDec(H(R, X, R^x), C_s), which may be $\perp$.

Security of stateful public-key scheme

This paper proved StDH is IND-CCA secure in the RO (Rondom oracle) model if Gap-DH holds. And StKD is also IND-CCA secure if DDH is supposed to be hard. The method used to prove both of them is the game playing technique. But one difference exists between the proof processes of StDH and StKD is, as for StKD, if the adversary sees secret key then it is asked to offer the pulbic key.

Conclusion

In this paper, a new stateful public-key sheme is proposed to speed-up the encryption part of the whole system, in which the encryption just cost 1 exponentiation that is less than 2 or 3 in the classic stateless public-key schemes, like DHIES and Kurosawa-Desmedt schemes. Besides, this new model does not increase the decryption part. And two new schemes, named StDH and StKD are put forward and the paper gave the proofs of security of the two schemes. They are both IND-CCA secure after applying game playing technique.