KASPERSKY lab

Schnorr Signcryption

Combining public key encryption with Schnorr digital signature

Laura Savu, University of Bucharest, Romania

"IT Security for the Next Generation"
European Cup, Prague
17-19 February, 2012

Kaspersky® Academy
IT Security
for the Next Generation
International Student Conference

Schnorr Signcryption

Signcryption is the primitive that has been proposed by Youliang Zheng in 1997 and it combines public key encryption and digital signature in a single logical step for obtaining less computational and communicational cost.

This article presents a new signcryption scheme which is based on the Schnorr algorithm. The new scheme has been implemented in a program and here are provided the steps of the algorithm, the results and some examples. In the end there are discussed the practical applications of Signcryption in real life.

Kill Two Birds with One Stone

Schnorr Signcryption

Data confidentiality and data integrity are two of the most important functions of modern cryptography. Confidentiality can be achieved using encryption algorithms or ciphers, whereas integrity can be provided by the use of authentication techniques. Encryption algorithms fall into one of two broad groups: private key encryption and public key encryption. Likewise, authentication techniques can be categorized by private key authentication algorithms and public key digital signatures.

Signcryption

Signcryption has the intention that the primitive should satisfy the condition

“Cost(Signature & Encryption) << Cost(Signature) + Cost(Encryption).”

This inequality can be interpreted in a number of ways:

- A signcryption scheme should be more computationally efficient than a native combination of public-key encryption and digital signatures.
- A signcryption scheme should produce a signcryption “ciphertext” which is shorter than a naive combination of a public-key encryption ciphertext and a digital signature.
- A signcryption scheme should provide greater security guarantees and/or greater functionality than a native combination of public-key encryption and digital signatures.

Signcryption

Signcryption Scheme

A signcryption scheme typically consists of five algorithms, Setup, KeyGenS, KeyGenR, Signcrypt, Unsigncrypt:

Setup - takes as input a security parameter 1^ *k* and outputs any common parameters *param* required by the signcryption schemes. This may include the security parameter 1^ k , the description of a group G and a generator g for that group, choices for hash functions or symmetric encryption schemes, etc.

Key Generation S(Gen) - generates a pair of keys for the sender

Key Generation R(Gen) - generates a pair of keys for the receiver

Signcryption (SC) - is a probabilistic algorithm

Unsigncryption (USC) - is a deterministic algorithm.

A signcryption scheme is a combination between a public key encryption algorithm and a digital signature scheme.

Schnorr Signcryption

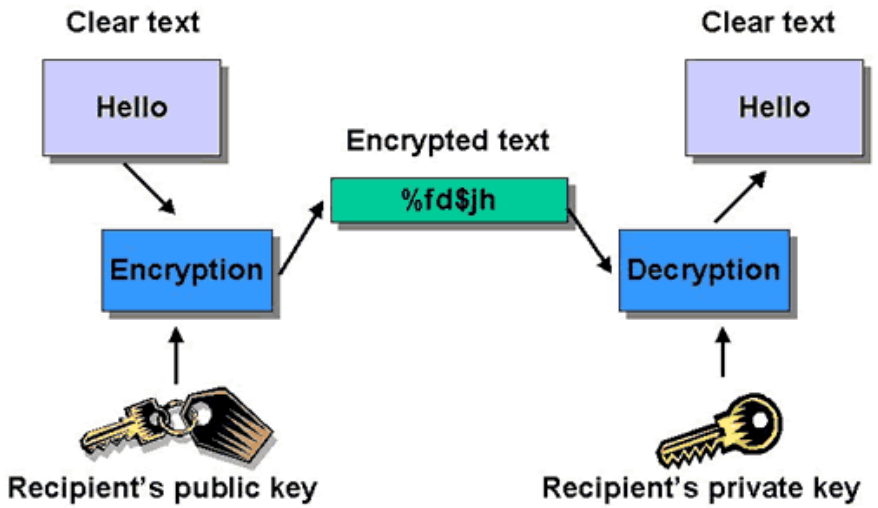
Public key encryption Scheme

A public key encryption scheme consists of three polynomial-time algorithms (EncKeyGen, Encrypt, Decrypt).

EncKeyGen - Key generation is a probabilistic algorithm that takes as input a security parameter and outputs a key pair (skenc, pkenc). The public encryption key pkenc is widely distributed, while the private decryption key skenc should be kept secret.

Encrypt - Encryption is a probabilistic algorithm that takes a message m ∈ M and the public key pkenc as input and outputs a ciphertext C ∈ C, written C ←Encrypt(pkenc,m)

Decrypt - Decryption is a deterministic algorithm that takes a ciphertext C ∈ C and the private key skenc as input and outputs either a message m ∈M or the failure symbol ⊥, written m ← Decrypt(skenc,C).



Signcryption – Related Work

ElGamal Signcryption

Based on discrete algorithm problem, ElGamal Signcryption cost is:

- **58%** less in average computation time
- **70%** less in message expansion

Here is the detailed presentation of the fifth algorithms that make up the ElGamal signcryption scheme.

1)Setup

Signcryption parameters:

p = a large prime number, public to all; q = a large prime factor of p-1, public to all; g = an integer with order q modulo p, in [1,… , p-1], public to all

hash = a one-way hash function; KH = a keyed one-way hash function = KHk(m) = hash(k, m)

(E, D) = the algorithms which are used for encryption and decryption of a private key cipher.

Alice sends a message to Bob.

2)KeyGen sender

Alice has the pair of keys (Xa, Ya):

Xa = Alice's private key, chosen randomly from [1, .., q-1]; Ya = Alice's public key = mod p

Signcryption – Related Work

ElGamal Signcryption

3)KeyGen receiver

Bob has the pair of keys(Xb, Yb):

Xb = Bob's private key, chosen randomly from [1, .., q-1]; Yb = Bob's public key = mod p.

4)Signcryption

In order to signcrypt a message m to Bob, Alice has to accomplish the following operations:

Calculate $k = hash(Yb^X) \bmod p$ Split k in k1 and k2 of appropriate length.

Calculate r = KHk2(m) = hash(k2, m).

Calculate s = x/(r+Xa) mod q, if SDSS1 is used

Calculate s = x/(1+Xa · r) mod q, if SDSS2 is used

Calculate c = Ek1(m) = the encryption of the message m with the key k1.

Alice sends to Bob the values (r, s, c).

5)Unsigncryption

In order to unsigncrypt a message from Alice, Bob has to accomplish the following operations:

Calculate k using r, s, g, p, Ya and Xb

$\text{hash}((Ya \cdot g^r)^{s \cdot Xb} \bmod p)$, if is used SDSS1

$\text{hash}((g \cdot Ya^r)^{s \cdot Xb} \bmod p)$, if is used SDSS2

Split k in k1 and k2 of appropriate length.

Calculate m using the decryption algorithm m = Dk1(c).

Accept m as a valid message only if KHk2(m) = r.

THE NEW SIGNCRYPTION SCHEME

Schnorr Signcryption

A Schnorr Signcryption scheme is based on Schnorr digital signature algorithm.

Here is the detailed presentation of the fifth algorithms that make up the Schnorr signcryption scheme.

1)Setup

Schnorr Signcryption parameters:

p = a large prime number, public to all

q = a large prime factor of p-1, public to all

g = an integer with order q modulo p, in [1,… , p-1], public to all

hash = a one-way hash function

KH = a keyed one-way hash function = KHk(m) = hash(k, m)

(E, D) = the algorithms which are used for encryption and decryption of a private key cipher.

Alice sends a message to Bob.

2)KeyGen sender

Alice has the pair of keys (Xa, Ya):

Xa = Alice's private key, chosen randomly from [1, .., q-1]

Ya = Alice's public key = mod p

THE NEW SIGNCRYPTION SCHEME

Schnorr Signcryption

3)KeyGen receiver

Bob has the pair of keys(Xb, Yb):

Xb = Bob's private key, chosen randomly from [1, .., q-1]

Yb = Bob's public key = mod p.

4)Signcryption

In order to signcrypt a message m to Bob, Alice has to accomplish the following operations:

Calculate $k = hash(Yb^X) \bmod p$

Split k in k1 and k2 of appropriate length.

Calculate r = KHk2(m) = hash(h2, m)

Calculate s = x + (r * Xa) mod q

Calculate c = Ek1(m) = the encryption of the message m with the key k1.

Alice sends to Bob the values (r, s, c).

5)Unsigncryption

In order to unsigncrypt a message from Alice, Bob has to accomplish the following operations:

Calculate k using r, s, g, p, Ya and Xb. Split k in k1 and k2 of appropriate length.

Calculate m using the decryption algorithm m = Dk1(c).

Accept m as a valid message only if KHk2(m) = r.

SECURITY MODELS FOR SIGNCRYPTION

Schnorr Signcryption

1) TWO-USERS SECURITY MODEL

In the symmetric setting, there is only one specific pair of users who

(1) share a single key;

(2) trust each other;

(3) “know who they are”;

(4) only care about being protected from “the rest of the world.”

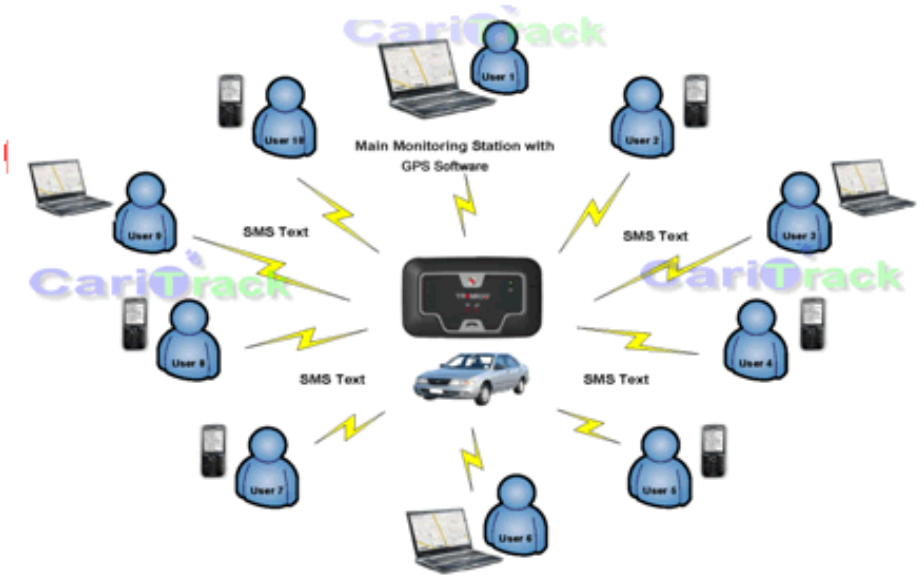
SECURITY MODELS FOR SIGNCRYPTION

Schnorr Signcryption

2) MULTI-USER SECURITY MODEL

A central difference between the multi-user model and the two-user models is the extra power of the adversary. In the multi-user model, the attacker may choose receiver (resp. sender) public keys when accessing the attacked users' signcryption (resp. unsigncryption) oracles. For signcryption schemes that share some functionality between the signature and the encryption components, such as are the case for Zheng's Signcryption scheme and Schnorr Signcryption scheme, the extra power of the adversary in the multi-user model may be much more significant, and a careful case-by-case analysis is required to establish security of such schemes in the multi-user model.

As in the two-user setting, the multi-user setting also has two types of models depending on the identity of the attacker: an insider model and an outsider model.



COMPARATIONAL RESULTS

Schnorr Signcryption

The Comparison between the proposed Schnorr Signcryption scheme and the initial Youliang Zheng Signcryption scheme.

	The Proposed Schnorr Signcryption Scheme	The Initial Youliang Zheng Signcryption Scheme
Computation cost for signature generation	Th + Tm	Th + Tm + Tinv
Computation cost for verifying converted signature	Th + Tm + Texp	Th + Tm + Tinv + Texp

- Texp: the time for a modular exponential computation
- Tm: the time for a modular multiplication computation
- Tinv: the time for a modular inverse computation
- Th: the time for a one way hash function f(_) computation

Schnorr Signcryption

Practical implementation of Signcryption in real life

The shared secret key between the parties makes possible an unlimited number of applications. Among these applications, one can first think of the following three:

- secure and authenticated key establishment,
- secure multicasting, and
- authenticated key recovery.

A number of signcryption-based security protocols have been proposed for aforementioned networks and similar environments. These include:

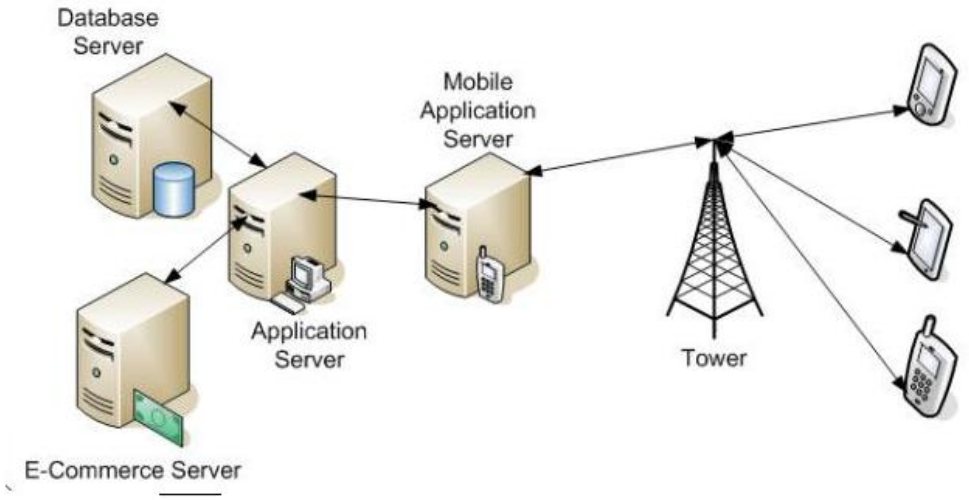
- secure ATM networks,
- secure routing in mobile ad hoc networks,
- secure voice over IP (VoIP) solutions,
- encrypted email authentication by firewalls,
- secure message transmission by proxy, and
- mobile grid web services.

Schnorr Signcryption

Practical implementation of Signcryption in real life

There are also various applications of signcryption in electronic commerce, where its security properties are very useful. Analyzing this security scheme from an application-oriented point of view, can be observed that a great amount of electronic commerce can take advantage of signcryption to provide efficient security solutions in the following areas:

- electronic payment,
- electronic toll collection system,
- authenticated and secured transactions with smart cards.



Thank You

Laura Savu, University of Bucharest, Romania

"IT Security for the Next Generation"

European Cup, Prague

17-19 February, 2012

KASPERSKY lab