Guillou Quisquater Protocol

Soumyadeep Basu, Kumar Utkarsh, Rohit Haolader, Raushan Raj, Suryasen Singh

V Semester BTech, Department of Information Technology,

Indian Institute of Information Technology, Allahabad, India.

Abstract

In cryptography, a zero-knowledge proof is a method by which one party (the prover) can prove to another party (the verifier) that they know a value x, without conveying any information apart from the fact that they know the value x. Many different schemes are there for this purpose and in this paper we will be discussing the Guillou Quisquater Protocol for this.

Introduction -- GQ identification scheme

A trusted center chooses a RSA integer n, product of two large and distinct primes p and q. It also selects a public RSA exponent v, that is an integer relatively prime with $\varphi(n) = (p - 1)(q - 1)$. We can assume that v is a small prime. The prover proves that they know the v^{th} root (1/B) modulo n of a given number J Є Z/nZ. The prover's public key is (J,v,n) and B is the private key.
The protocol works as follows :

- 1. Prover chooses a random number $r \in \{1, 2, ..., n - 1\}$ and computes $T \equiv r^v[n]$. The result is then sent to the verifier.
- 2. Verifier chooses a random number $d \in \{0, 1, .., v - 1\}$ and sends it to Prover.
- 3. Prover replies by sending $t \equiv r.B^d [n]$.

Since the protocol is an honest-verifier zero knowledge, it follows easily that it is secure against impersonation under passive attack. This is based on the assumption that RSA is one way.
The main question is whether the protocol is secure against impersonation under active attack. No attack has been found. However, no proof of security has been provided either. Furthermore, it is difficult to imagine such a proof being based solely on the assumption that RSA is one-way. In other words, the protocol seems to be secure against impersonation under active attack, but due to properties of RSA that go beyond mere one-wayness.

Method

With the GQ method, Peggy (the prover) has a proving public key of (N,e,X) and a proving secret key of (N,x). N is a prime number for the modulus operation. In this case x is the secret, and where:

$X=x^e(\text{mod}N)$
On the registration of the secret, Peggy generates a random value (y), and then computes Y:

$Y \leftarrow y^e(\text{mod}N)$
This value is sent to Victor (who is the verifier). Victor then generates a random value (c) and sends this to Peggy. This is a challenge to Peggy to produce the correct result. Peggy then computes:

$z \leftarrow yx^c(\text{mod}N)$
She then sends this to Victor in order to prove that she knows x. Victor then computes two values:

$val1=YX^c(\text{mod}N)$
$val2=X^e(\text{mod}N)$
If the values are the same (val1≡val2), Peggy has proven that she knows x.

This works because:
$YX^c=y^e(x^e)^c=y^ex^{ec}$
$z^e=(yx^c)^e=y^ex^{ec}$

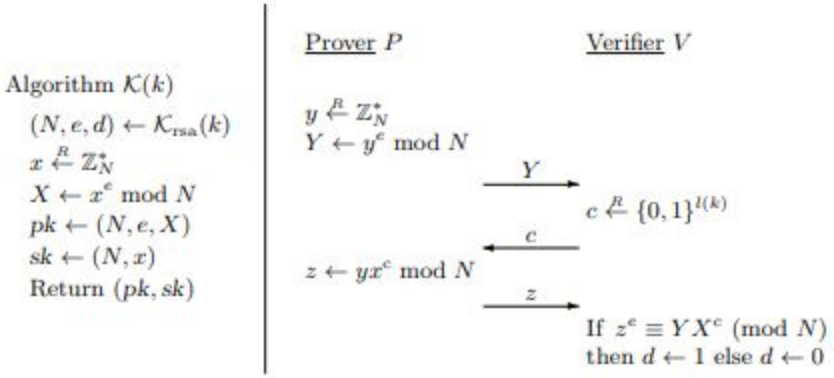

Fig:- GQ identification scheme. Prover P has input pk = (N, e, X) and sk = (N, x). Verifier V has input pk.

Security Analysis

Assume that Oscar is an attacker.

- Attack 1 : Knowing Alice public key. If Oscar intercepts the value of d and t, then he can compute the scalar T using the equation, but it does not work, because he must send the value of T at the beginning of the procedure.
- Attack 2 : Even if the attacker intercepts the value of t he is not able to find Alice's secret key, because he must solve the equation with two unknowns B and r.
- Attack 3 : Suppose that the attacker intercepts the value of T and t. If he tries to imitate the identification of Alice, then he will be blocked at the challenge number d which is changeable at each identification.

Hence , through this brief security analysis, it can be concluded that the attacker cannot break the GQ System easily.

Conclusions

In this paper we have described the Guillou-Quisquater Protocol which is based on the concept of zero-knowledge proof and analyzed it's security along with the algorithm it uses for this security. Although it is quite strong, but still it has certain limitations due to RSA's assumed one-wayness.

References

1. M. Abdalla, J. An, M. Bellare and C. Namprempre. From identification to signatures via the Fiat-Shamir Transform: Minimizing assumptions for security and forward-security. Advances in Cryptology – EUROCRYPT '02, Lecture Notes in Computer Science Vol. 2332 , L. Knudsen ed., Springer-Verlag, 2002.

2. M. Bellare, M. Fischlin, S. Goldwasser and S. Micali. Identification protocols secure against reset attacks. Advances in Cryptology – EUROCRYPT '01, Lecture Notes in Computer Science Vol. 2045, B. Pfitzmann ed., Springer-Verlag, 2001.

3. M. Bellare and S. Miner. A forward-secure digital signature scheme. Advances in Cryptology – CRYPTO '99, Lecture Notes in Computer Science Vol. 1666, M. Wiener ed., Springer-Verlag, 1999.