On the Soundness of Girault's Scheme

Fabrice BOUDOT
France Télécom R&D
42, rue des coutures - BP6243
14066 Caen Cedex 4
France
Tel. +33 2 31 75 92 68
Email: fabrice.boudot@francetelecom.fr

28 April 2000

The Girault protocol [Eurocrypt'91] is a zero-knowledge like scheme which allows Alice to prove to Bob that she knows x, a discrete logarithm of y in base g modulo n, where n is a composite number whose factorization is unknown. It runs as follows: Alice randomly selects $r \in [0, A]$ (where $A \gg n$) and sends $W = g^r \bmod n$ to Bob. Bob sends to Alice a random challenge $c \in [0, k]$. Alice sends in reply $D = r + xc(inZ)$. Bob accepts the proof if $W = g^D y^{-c} \bmod n$.

Poupard and Stern [Eurocrypt'98] prove that this protocol is sound if computing discrete logarithms modulo n is hard, but *only when this protocol is used for identification or signature schemes*, i.e. when an attacker cannot choose the public data y. For other contexts (when an attacker can choose the public data y), Fujisaki and Okamoto [Crypto'97] "prove" that this protocol is sound if the strong RSA assumption holds, i.e. an attacker cannot succeeds if he does not know a discrete logarithm of y.

We show that Fujisaki-Okamoto's claim is wrong, and hence so is their proof. Moreover, an attacker can succeed to Girault's protocol without knowing the discrete logarithm of y: he can succeed with probability 1/2 if he only knows the discrete logarithm of $-y$ in base g modulo n[1]: if c is even, the attacker replies $D = r + x'c$, where x' is the discrete logarithm of $-y$.

To design a sound protocol, we slightly transform Girault's protocol into a zero-knowledge like proof of knowledge of a discrete logarithm of $\pm y$ in base g modulo n. Moreover, we prove that this protocol is sound if the RSA assumption holds (instead of the strong RSA assumption).

[1]Note that when the factorization of n is unknown, the knowledge of a discrete logarithm of $-y$ does not allow to compute a discrete logarithm of y (it is not the case if n is prime or when the factorization of n is known). Moreover, the knowledge of discrete logarithms of y and $-y$ allows to factor n.