

Important Note on “Certificateless Public Key Encryption without Pairing”

Joonsang Baek

April 13, 2007

Recently Yingxia Sun (Bela Suno)¹ pointed out that “[Simulation of Phase I-3]” of the proof of Lemma 1 does not consider the case when the Type-I attacker A_I possibly replaces the public key $(w^*, \mu^*)(= (g^{s^*}, g^{z^*}))$ associated with the target identity ID^* with its own $(w, \mu)(= (g^s, g^z))$. When $s \neq s^*$, the CDH attack algorithm B simulating the environment of A_I may not know s and hence has no way to find the Diffie-Hellman key at the end of the simulation and hence fails to solve the CDH problem.

Thus the security proof of the proposed CLPKE scheme only holds for the weaker security model in which the Type-I attacker A_I is not allowed to replace the public key associated with the target identity ID^* , or the model in which A_I conducts “limited public key replacement attack” where A_I does not replace the first component w^* of the public key associated with ID^* . Alternatively one may define a new computational assumption which is related to the CDH but is non-standard.

A solution that fixes this problem without altering underlying security or computational assumption has yet to be found...

¹The author is grateful to him/her for reading the security proof very carefully.