

[] ITU-T 가

ITU-T SG17 WP2 9 , , , 5 가

ITU-T SG17 . ITU-T SG17 9
(SPAK: Secure Password -based Authentication Protocol
with Key exchange) 가 , 5 SPAK
PAK(Password-Authenticated Key Exchange) .

, 2005 10 가
가 , 1
가
, 5 PAK 가 1 SG17 WP2

,
가 (), (),
가 ()

.
가 ,
가
, 가 ,

DH(Diffie - Hellman) ,
가
가
, ,

, 가
가 (dictionary attack)

가
(Phishing)

가

가

PAK

가 가

2005 10 2006 2 ITU-T SG17

가

가

9

가

9

가

PAK

가

2

5

Z.Zeltsan(

)

(

, hyyoum@sch.ac.kr)