A Provably Secure General Construction for Key Exchange Protocols Using Smart Card and Password*

ABSTRACT:

Key exchange protocols using both smart card and password are widely used nowadays since they provide greater convenience and stronger security than protocols using only a password. Most of these protocols are often limited to simple network systems, and they may have security risks. We propose a general construction for key exchange protocols using smart card and password to avoid these flaws. The constructed protocol from the general construction has only one additional communication round than the original public encryption scheme. This construction is proven secure under random oracle model, so it can resist several common types of attacks. It is also adapted well to various networks. Compared with related protocols, the proposed key exchange protocol generated from the general construction has better secure properties and good computational efficiency in storage cost and operation time.

SHIELD TECHNOLOGIES,

2232, 3RD FLOOR, 16TH B CROSS, YELAHANKA NEW TOWN, BANGALORE-64

Mail us: shieldtechnoblr@gmail.com / manager@shieldtechno.com

Contact: 9972364704 / 8073744810