**MPS[[1]](#footnote-2) Protocol – BAN logic**

**Sign Up Real Protocol**

: A → S:

: S → A: ||

: A → S:

: S → A:

**Sign Up Idealized Protocol**

: A → S:

: S → A: ||

: A → S:

: S → A:

**Sign Up Protocol Analysis**

**Objectives**

# Diffie Hellman Parameters

# Symmetric Key

**Assumptions**

# Hardcoded Server’s Public Key

# Alice’s Public Key sent in plaintext in the first message

# Symmetric Key

After :

After :

After :

After :

**Authentication Real Protocol**

: A → S:

: S → A:

: A → S:

**Authentication Idealized Protocol**

: A → S:

: S → A:

: A → S:

**Authentication Analysis**

**Objectives**

, # Session ID Establishing

**Assumptions**

# Key Registration

# Nonce Authority

After :

After :

After :

**Online Key Exchange Real Protocol**

: A → S:

: S → A:

: A → B: ||

: B → A: ||

: A → B:

: A → B:

**Online Key Exchange Idealized Protocol**

: A → S:

: S → A:

: A → B: ||

: B → A: ||

: A → B:

**Online Key Exchange Analysis**

**Objectives**

, # Key Authentication

, # Key Confirmation

**Assumptions**

, # Symmetric keys

, # Symmetric keys

# Freshness of the session ids used during the authentication protocol

, ,

# Diffie Hellman’s parameters

# Authority on Y parameters

After :

After :

After :

After :

After :

**Offline Communication Real Protocol**

: A → S:

: S → A:

: A → S: ||

**Offline Communication Idealized Protocol**

: A → S:

: S → A:

**Offline Communication Analysis**

**Objective**

# Bob’s Public Key

**Assumptions**

, # Symmetric keys

# Freshness of the session id used during the authentication protocol

,

After :

After :

1. Magherini – Pochiero – Sieni (MPS) [↑](#footnote-ref-2)