**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

# DH Parameters confirmation

**Assumptions**

# Hardcoded Server’s Public Key

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

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

# Session Key

# Session Key confirmation

**Assumptions**

# Session Key

# Hardcoded Server’s Public Key

# Alice’s Public Key

# Nonce Authority

# Session Key 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**

, # A-S Session keys (authentication protocol)

, # B-S Session keys (authentication protocol)

, , # Freshness session ids (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:

: S → B:

**Offline Communication Idealized Protocol**

: A → S:

: S → A:

**Offline Communication Analysis**

**Objective**

# Bob’s Public Key

**Assumptions**

, # Session key (authentication protocol)

, # Freshness session ids (authentication protocol)

After :

After :

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