PETIKAN LOGIKA TERHADAP VERIFIKASI FORMAL
“PROTOCOL Crypto-0N2 WITH THE BLIND SCHNORR
SIGNATURE SCHEME IMPLEMENTATION“

Esti Rahmawati Agustina¹, Ikhsan Budiarsro²
Lembaga Sandi Negara¹²
esti.rahmawati@lemsaneg.go.id¹
ikhsan.budiarsro@lemsaneg.go.id²

ABSTRAK


Kata-kata kunci: e-voting, protokol Crypto-0N2, The Blind Schnorr Signature Scheme, pemekatan logika, BAN Logic, kriptografi

PENDAHULUAN


663

PENELITIAN SEBELUMNYA

PROTOKOL “CryptO-0N2 with The Blind Schnorr Signature Scheme Implementation”
Protokol “CryptO-0N2 with The Blind Schnorr Signature Scheme Implementation” terdiri dari 2 (dua) proses, yaitu proses otentikasi dan tabulasi. Proses otentikasi merupakan proses verifikasi untuk memeriksa apakah pemilih merupakan pemilih yang sah, sedangkan proses tabulasi adalah proses perhitungan suara pilihan pemilih. Pada protokol ini diperlukan 2 (dua) server yaitu server otentikasi dan server tabulasi. Skema protokol CryptO-0N2 with The Blind Schnorr Signature Scheme Implementation terlihat pada Gambar 1. Rincian penjelasan protokol CryptO-0N2 with The Blind Schnorr Signature Scheme Implementation terdapat pada Lampiran A.
Gambar 1. Protokol CRYPTO-0N2 with The Blind Schnorr Signature Scheme Implementation

Tabel 1. Simbol Properti dan Artinya pada Protokol CRYPTO-0N2 with The Blind Schnorr Signature Scheme Implementation

<table>
<thead>
<tr>
<th>Simbol Properti</th>
<th>Arti</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Identitas pemilihan</td>
</tr>
<tr>
<td>(N, num)</td>
<td>Identification number</td>
</tr>
<tr>
<td>T_e</td>
<td>Timestamps</td>
</tr>
<tr>
<td>K_e</td>
<td>Kunci publik Tempat Pemungutan Suara (TPS)</td>
</tr>
<tr>
<td>K_s</td>
<td>Kunci Publik Server Otentikasi</td>
</tr>
<tr>
<td>K_e^-1</td>
<td>Kunci privat Tempat Pemungutan Suara (TPS)</td>
</tr>
<tr>
<td>K_e^-2</td>
<td>Kunci Privat Server Otentikasi</td>
</tr>
<tr>
<td>K_t</td>
<td>Kunci publik server tabulasi</td>
</tr>
<tr>
<td>p, q, r</td>
<td>Parameter untuk proses pembuatan (blinding) pesan oleh TPS</td>
</tr>
<tr>
<td>s</td>
<td>Pesan buta yang dibuat oleh TPS</td>
</tr>
<tr>
<td>s</td>
<td>Pesan buta yang telah ditandatangani oleh server penandatangans</td>
</tr>
<tr>
<td>m dan a', s'</td>
<td>Pesan dan tanda tangan yang berkorespondensi</td>
</tr>
<tr>
<td>r</td>
<td>Parameter untuk proses verifikasi</td>
</tr>
<tr>
<td>H</td>
<td>Fungsi Hash</td>
</tr>
<tr>
<td>i</td>
<td>Concate</td>
</tr>
</tbody>
</table>

METODE
Pada makalah ini metode yang digunakan adalah Tipe III dengan menggunakan BAN Logic. Langkah-langkah analisis protokol menggunakan metode BAN Logic adalah:
- a. Membentuk protokol yang idealis dari protokol aslinya.
- b. Memberikan asumsi pada bentuk idealis dari langkah sebelumnya.
- c. Logical formula ditambahkan pada setiap pernyataan protokol, sebagai penegasan dalam setiap pernyataan protokol.
- d. Logical postulate diaplikasikan dari langkah kedua dan ketiga untuk menemukan kepercayaan antara pihak dalam protokol.
Pada BAN logic digunakan notasi – notasi untuk mempermudah proses analisis. Berikut notasi dan pengertianannya pada Tabel 2:

<table>
<thead>
<tr>
<th>Notasi</th>
<th>Pengertian</th>
</tr>
</thead>
<tbody>
<tr>
<td>P ⊨ X</td>
<td>P akan percaya X, P yakin bahwa X benar</td>
</tr>
<tr>
<td>P ⊬ X</td>
<td>Seseorang telah mengirimkan pesan berisi X kepada P</td>
</tr>
<tr>
<td>P ⊸ X</td>
<td>P telah mengirimkan pesan berisi pernyataan X</td>
</tr>
<tr>
<td># (X)</td>
<td>Formula X adalah fresh artinya belum pernah dikerim dalam pesan sebelum protokol yang sedang berjalan</td>
</tr>
<tr>
<td>K → A</td>
<td>A memiliki kunci publik K, inverse K dari yaitu K^(-1)</td>
</tr>
</tbody>
</table>
Berikut adalah aturan-aturan dalam pendekatan BAN Logic [12]:

   1) Untuk shared key dipostulaskan:
      \[ P \equiv Q \leftrightarrow P, P \equiv \langle X \rangle_X \]
      Aturan tersebut mempunyai arti P percaya kunci K telah dipertukarkan antara Q dan P dan hanya keduanya yang mengetahui K dan P menerima pesan X yang dienkripsi menggunakan kunci K sehingga P percaya bahwa Q telah mengirimkan pesan X.
   2) Untuk kunci publik dipostulaskan:
      \[ P \equiv K \leftrightarrow Q, P \equiv \langle X \rangle_{K^{-1}} \]
      Aturan tersebut mempunyai arti bahwa P percaya bahwa Q mempunyai kunci public K dan P telah menerima pesan X yang dienkripsi menggunakan kunci K^{-1}, yaitu kunci privasi Q sehingga P percaya bahwa Q telah mengirimkan pesan X.

b. Aturan nonce-verification. Aturan ini memerlika apakah pesan terkini/tidak, dipostulaskan:
   \[ P \equiv \#(X), P \equiv Q \leftrightarrow X \]
   Aturan tersebut mempunyai arti bahwa P percaya pesan X adalah fresh dan P percaya Q telah mengirimkan X sehingga P percaya Q percaya X.

c. Aturan on hashing, dipostulaskan:
   \[ P \equiv Q \leftrightarrow H(X), P \equiv Q \leftrightarrow X \]
   Aturan tersebut mempunyai arti bahwa P percaya bahwa Q telah mengirimkan nilai hash dari pesan X dan P telah menerima X sehingga P percaya bahwa Q telah mengirimkan X.

ANALISIS PROTOKOL “Crypto-0N2 with The Blind Schnorr Signature Scheme Implementation”
Analisis terhadap protokol “Crypto-0N2 with The Blind Schnorr Signature Scheme Implementation” dilakukan dengan menggunakan pendekatan BAN Logic. Analisis ini dilakukan mengikuti langkah-langkah yang telah diemukakan pada bab sebelumnya. Berikut adalah analisisnya:

a. Membentuk protokol idealis dari protokol aslinya.
Mengidealkan protokol berarti menyederhanakan properti yg tidak diproses karena tidak mempengaruhi hasil analisis selanjutnya, misalnya identitas bisa dihilangkan, tetapi properti seperti Nonce, Timestamp, dan kunci sesi tidak boleh dihilangkan. Berikut adalah tabel 3 yang menunjukkan perubahan bentuk asli ke bentuk idealis:

<table>
<thead>
<tr>
<th>Pesan ke-x</th>
<th>Bentuk Asli</th>
<th>Bentuk Idealis</th>
</tr>
</thead>
<tbody>
<tr>
<td>A \rightarrow S</td>
<td>{(id, iNum, T_e) \mid H_e x }</td>
<td>{(M_a, T_e, H_e x) }</td>
</tr>
<tr>
<td>S \rightarrow A</td>
<td>{(id, T_e+1, p, q, g, r) \mid H_e x }</td>
<td>{(M_a, T_e+1, H_e x) }</td>
</tr>
<tr>
<td>A \rightarrow S</td>
<td>{(s, T_e+2, H_e x) \mid H_e x }</td>
<td>{(M_a, T_e+2, H_e x) }</td>
</tr>
<tr>
<td>S \rightarrow A</td>
<td>{(s, T_e+3, H_e x) \mid H_e x }</td>
<td>{(M_a, T_e+3, H_e x) }</td>
</tr>
<tr>
<td>A \rightarrow T</td>
<td>{(m, r', s', H(T_e+4, H_e x) \mid H_e x }</td>
<td>{(M_a, H(T_e+4, H_e x) }</td>
</tr>
<tr>
<td>T \rightarrow A</td>
<td>{(H(T_e+5, H_e x) \mid H_e x }</td>
<td>{(H(T_e+5, H_e x) }</td>
</tr>
</tbody>
</table>

A adalah Tempat Penyungatan Suara, S adalah server otentikasi, dan T adalah server tabulasi suara. Pada protokol bentuk idealis M_1 bernilai identitas dan iNum karena iNum digunakan untuk melakukan autentikasi terhadap data base pada server bahwa identitas tersebut telah terdaftar pada data base sehingga setelah pasti pemilih terdaftar pada server, M_2 pada pesan 2 hanya berisi identitas dari pemilih tersebut. M_2 adalah e, M_3 adalah s, M_4 adalah m, e', s' dan M_5 adalah r'.

b. Memberikan asumsi pada setiap langkah protokol yaitu pada setiap pesan.
Pemberian asumsi ini berdasarkan pada properti yang digunakan dalam protokol yaitu kunci publik, kunci privat dan timestamp. Tabel berikut menunjukkan properti yang digunakan serta asumsi dan penjelasannya:
<table>
<thead>
<tr>
<th>Grup Pertama</th>
<th>Penjelasan</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A \equiv K_A \rightarrow A$</td>
<td>A percaya bahwa $K_A$ merupakan kunci publik dari $A$ sehingga $A$ harus mempunyai kunci privat ($K_A^{-1}$)</td>
</tr>
<tr>
<td>$A \equiv K_A \rightarrow S$</td>
<td>A percaya bahwa $K_A$ merupakan kunci publik dari $S$ sehingga $S$ harus mempunyai kunci privat ($K_A^{-1}$)</td>
</tr>
<tr>
<td>$S \equiv K_A \rightarrow S$</td>
<td>S percaya bahwa $K_A$ merupakan kunci publik dari $S$ sehingga $S$ harus mempunyai kunci privat ($K_A^{-1}$)</td>
</tr>
<tr>
<td>$S \equiv K_A \rightarrow A$</td>
<td>S percaya bahwa $K_A$ merupakan kunci publik dari $A$ sehingga $A$ harus mempunyai kunci privat ($K_A^{-1}$)</td>
</tr>
<tr>
<td>$T \equiv K_T \rightarrow A$</td>
<td>T percaya bahwa $K_T$ merupakan kunci publik dari $A$ sehingga $T$ harus mempunyai kunci privat ($K_T^{-1}$)</td>
</tr>
<tr>
<td>$T \equiv K_T \rightarrow S$</td>
<td>T percaya bahwa $K_T$ merupakan kunci publik dari $S$ sehingga $T$ harus mempunyai kunci privat ($K_T^{-1}$)</td>
</tr>
<tr>
<td>$A \equiv K_A \rightarrow T$</td>
<td>A percaya bahwa $K_A$ merupakan kunci publik dari $T$ sehingga $T$ harus mempunyai kunci privat ($K_A^{-1}$)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Grup Kedua</th>
<th>Penjelasan</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S' \equiv # (M_2)$</td>
<td>Dari grup kedua diasumsikan bahwa pesan yang dikirimkan bersamaan dengan timestamp menunjukkan bahwa pesan tersebut adalah fresh. Dengan asumsi ini, setiap entitas dalam protokol percaya bahwa setiap langkah dalam protokol tidak mengirimkan informasi yang sama dengan langkah sebelumnya. Hal ini didasarkan karena penggunaan timestamp yang nilainya selalu berbeda</td>
</tr>
<tr>
<td>$A' \equiv # (M_2)$</td>
<td></td>
</tr>
<tr>
<td>$S' \equiv # (M_2)$</td>
<td></td>
</tr>
<tr>
<td>$A' \equiv # (M_2)$</td>
<td></td>
</tr>
</tbody>
</table>

### Tabel 5. Logical Formula pada Setiap Pesan

<table>
<thead>
<tr>
<th>Pesan $k_e$</th>
<th>Logical Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pesan 1</strong></td>
<td>$A \rightarrow S$</td>
</tr>
<tr>
<td></td>
<td>${[M_1, T_1] K_e^{-1} K_a}$</td>
</tr>
</tbody>
</table>

Pesan 1 berarti $S$ telah menerima pesan $M_1$ dan $T_1$ dari $A$. Kedua properti ini ditandatangani dengan menggunakan kunci privat milik $A$, $K_a^{-1}$. Logical formulanya adalah sebagai berikut:

$S \equiv \{M_1, T_1\} K_e^{-1}$.

Selain itu penggunaan timestamp pada pesan 1 menunjukkan bahwa pesan $M_1$ belum pernah dikirimkan sebelum protokol berjalan. Jadi Logical formulanya adalah sebagai berikut:

$S \equiv A \rightarrow M_1$.

| **Pesan 2** | $S \rightarrow A$ |
| | $\{[M_1, T_1+1] K_e^{-1} K_a\}$ |

Pesan 2 berarti $A$ telah menerima pesan $M_1$ dan $T_{e+1}$ dari $S$. Kedua properti ini ditandatangani dengan menggunakan kunci privat milik $S$, $K_e^{-1}$. Logical formulanya adalah sebagai berikut:

$A \equiv \{M_1, T_{e+1}\} K_e^{-1}$.

Selain itu penggunaan timestamp plus 1 pada pesan 2 menunjukkan bahwa pesan $M_1$ belum pernah dikirimkan sebelum protokol berjalan. Jadi Logical formulanya adalah sebagai berikut:

$A \equiv S \rightarrow M_1$.

| **Pesan 3** | $A \rightarrow S$ |
| | $\{[M_2, T_2] K_e^{-1} K_a\}$ |

Pesan 3 berarti $S$ telah menerima pesan $M_2$ dan $T_2$ dari $A$. Kedua properti ini ditandatangani dengan menggunakan kunci privat milik $A$, $K_a^{-1}$. Logical formulanya adalah sebagai berikut:

$S \equiv \{M_2, T_2\} K_e^{-1}$.

Selain itu penggunaan timestamp pada pesan 3 menunjukkan bahwa pesan $M_2$ belum pernah dikirimkan sebelum protokol berjalan. Jadi Logical formulanya adalah sebagai berikut:

$S \equiv A \rightarrow M_2$.

| **Pesan 4** | $S \rightarrow A$ |
| | $\{[M_2, T_2+2] K_e^{-1} K_a\}$ |

Pesan 4 berarti $A$ telah menerima pesan $M_2$ dan $T_{e+2}$ dari $S$. Kedua properti ini ditandatangani dengan menggunakan kunci privat milik $S$, $K_e^{-1}$. Logical formulanya adalah sebagai berikut:

$S \equiv S \rightarrow M_2$.
Pesan 4 berarti A telah menerima pesan \( M_2 \) dan \( T_{e+3} \) dari S. Kedua properti ini ditandatangani dengan menggunakan kunci privil melik S, \( K_{e}^{-1} \). Logical formulanya adalah sebagai berikut:

\[
A \Leftarrow \{ M_2, T_{e+3} \} K_{e}^{-1}
\]

Selain itu penggunaan timestamp pada pesan 4 menunjukkan bahwa pesan \( M_2 \) belum pernah dikirimkan sebelum protokol berjalan. Jadi Logical formulanya adalah sebagai berikut:

\[
S \equiv A \Rightarrow M_2
\]

### Pesan 5

\[
A \Rightarrow T \\
\{ M_4, M_5, H(T_{e+4} || M_5) \} K_{e}^{-1}
\]

Pesn 5 berarti T telah menerima pesan \( M_4 \) dan \( H(T_{e+4} || M_5) \) dari A. Kedua properti ini ditandatangani dengan menggunakan kunci privil melik A, \( K_{e}^{-1} \). Logical formulanya adalah sebagai berikut:

\[
T \Leftarrow \{ M_4, M_5, H(T_{e+4} || M_5) \} K_{e}^{-1}
\]

Selain itu penggunaan timestamp pada pesan 5 menunjukkan bahwa pesan \( M_4 \) dan \( M_5 \) belum pernah dikirimkan sebelum protokol berjalan. Jadi Logical formulanya adalah sebagai berikut:

\[
T \equiv A \Rightarrow M_4 \\
T \equiv A \Rightarrow M_5
\]

### Pesan 6

\[
T \Rightarrow A \\
\{ H(T_{e+5} || M_5) \} K_{e}^{-1}
\]

Pesn 6 berarti A telah menerima pesan \( H(T_{e+5} || M_5) \) dari T. Kedua properti ini ditandatangani dengan menggunakan kunci privil melik T, \( K_{e}^{-1} \). Logical formulanya adalah sebagai berikut:

\[
A \Leftarrow \{ H(T_{e+5} || M_5) \} K_{e}^{-1}
\]

Selain itu penggunaan timestamp pada pesan 6 menunjukkan bahwa pesan \( M_5 \) belum pernah dikirimkan sebelum protokol berjalan. Jadi Logical formulanya adalah sebagai berikut:

\[
S \equiv A \Rightarrow M_5
\]

d. Mengaplikasikan langkah kedua dan langkah ketiga untuk menemukan kepercayaan antar pihak dalam protokol. Terdapat tiga pihak dalam protokol ini yaitu Tempat Pemungutan Suara (TPS), Server Otentikasi, dan Server Tabulasi.

1) Menemukan kepercayaan antar pihak dalam penggunaan kunci publik

Notasi yang digunakan yaitu

\[
P \equiv 0, Q \equiv \{ x_{-1} \}, P \equiv Q \equiv X
\]

namun disesuaikan dengan properti yang ada pada setiap pesan.

Untuk pesan 1 maka notasinya menjadi

\[
S \equiv A \Rightarrow S, A \equiv \{ M_2, T_{e+3} \} K_{e}^{-1}
\]

Untuk pesan 2 maka notasinya menjadi

\[
A \equiv B \Rightarrow S, A \equiv \{ M_2, T_{e+3} \} K_{e}^{-1}
\]

Untuk pesan 3 maka notasinya menjadi

\[
S \equiv A \Rightarrow S, A \equiv \{ M_2, T_{e+3} \} K_{e}^{-1}
\]

Untuk pesan 4 maka notasinya menjadi

\[
A \equiv B \Rightarrow S, A \equiv \{ M_2, T_{e+3} \} K_{e}^{-1}
\]

Untuk pesan 5 maka notasinya menjadi

\[
T \equiv A \Rightarrow S, A \equiv \{ M_2, T_{e+3} \} K_{e}^{-1}
\]

Untuk pesan 6 maka notasinya menjadi

\[
T \equiv A \Rightarrow S, A \equiv \{ M_2, T_{e+3} \} K_{e}^{-1}
\]

Berikut adalah Tabel 6 yang menunjukkan aplikasi dari langkah kedua dan ketiga.

<table>
<thead>
<tr>
<th>Pesan ke-x</th>
<th>Asumsi (dari langkah kedua)</th>
<th>Logical Formula (dari langkah ketiga)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( A \Rightarrow S )</td>
<td>( S \equiv { M_2, T_{e+3} } K_{e}^{-1} )</td>
</tr>
<tr>
<td>2</td>
<td>( S \Rightarrow A )</td>
<td>( A \equiv { M_2, T_{e+3} } K_{e}^{-1} )</td>
</tr>
<tr>
<td>3</td>
<td>( A \Rightarrow S )</td>
<td>( S \equiv { M_2, T_{e+3} } K_{e}^{-1} )</td>
</tr>
<tr>
<td>4</td>
<td>( A \Rightarrow S )</td>
<td>( A \equiv { M_2, T_{e+3} } K_{e}^{-1} )</td>
</tr>
<tr>
<td>5</td>
<td>( T \Rightarrow A )</td>
<td>( T \equiv { M_2, T_{e+3} } K_{e}^{-1} )</td>
</tr>
</tbody>
</table>

a) Antara Tempat Pemungutan Suara (TPS) dan Server Otentikasi.

**Pesn 1**

Notasi yang akan dipenuhi adalah
\[ S \equiv \{ A, S = \{ M_1, T_0 \}_K_{-1} \} \]
\[ S \equiv A \sim \{ M_2, T_2 \}_K_{-1} \]
Kondisi \( S \equiv A \sim \{ M_1, T_0 \}_K \) akan dipenuhi jika kondisi \( S \equiv \{ A \} \) dan \( S \equiv \{ M_1, T_0 \}_K \) dipenuhi.
Dari tabel 6 didapatkan informasi bahwa kedua kondisi tersebut telah dipenuhi. Sehingga dapat diambil kesimpulan bahwa dalam penggunaan kunci publik pada pesan pertama telah memenuhi notasi.

**Pesan 2**

Notasi yang akan dipenuhi adalah
\[ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \]
\[ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \]
Kondisi \( A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \) akan dipenuhi jika kondisi \( A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \) dipenuhi.
Dari tabel 6 didapatkan informasi bahwa kedua kondisi tersebut telah dipenuhi. Sehingga dapat diambil kesimpulan bahwa dalam penggunaan kunci publik pada pesan kedua telah memenuhi notasi.

**Pesan 3**

Notasi yang akan dipenuhi adalah
\[ S \equiv \{ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \} \]
\[ S \equiv \{ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \} \]
Kondisi \( S \equiv \{ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \} \) akan dipenuhi jika kondisi \( S \equiv \{ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \} \) dipenuhi.
Dari tabel 6 didapatkan informasi bahwa kedua kondisi tersebut telah dipenuhi. Sehingga dapat diambil kesimpulan bahwa dalam penggunaan kunci publik pada pesan ketiga telah memenuhi aturan.

**Pesan 4**

Notasi yang akan dipenuhi adalah
\[ A \equiv \{ S \equiv \{ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \} \} \]
\[ A \equiv \{ S \equiv \{ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \} \} \]
Kondisi \( A \equiv \{ S \equiv \{ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \} \} \) akan dipenuhi jika kondisi \( A \equiv \{ S \equiv \{ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \} \} \) dipenuhi.
Dari tabel 6 didapatkan informasi bahwa kedua kondisi tersebut telah dipenuhi. Sehingga dapat diambil kesimpulan bahwa dalam penggunaan kunci publik pada pesan keempat telah memenuhi aturan.

b) Antara Tempat Pemungutan Suara (TPS) dan Server Tabulasi

**Pesan 5**

Notasi yang akan dipenuhi adalah
\[ T \equiv \{ A \equiv \{ S \equiv \{ M_2, M_3, H(T_2 + 4) \}_K \}_K_{-1} \} \]
\[ T \equiv \{ A \equiv \{ S \equiv \{ M_2, M_3, H(T_2 + 4) \}_K \}_K_{-1} \} \]
Kondisi \( T \equiv \{ A \equiv \{ S \equiv \{ M_2, M_3, H(T_2 + 4) \}_K \}_K_{-1} \} \) akan dipenuhi jika kondisi \( T \equiv \{ A \equiv \{ S \equiv \{ M_2, M_3, H(T_2 + 4) \}_K \}_K_{-1} \} \) dipenuhi.
Dari tabel 6 didapatkan informasi bahwa kedua kondisi tersebut telah dipenuhi. Sehingga dapat diambil kesimpulan bahwa dalam penggunaan kunci publik pada pesan kelima telah memenuhi aturan.

**Pesan 6**

Notasi yang akan dipenuhi adalah
\[ A \equiv \{ T \equiv \{ S \equiv \{ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \} \} \} \]
\[ A \equiv \{ T \equiv \{ S \equiv \{ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \} \} \} \]
Kondisi \( A \equiv \{ T \equiv \{ S \equiv \{ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \} \} \} \) akan dipenuhi jika kondisi \( A \equiv \{ T \equiv \{ S \equiv \{ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \} \} \} \) dipenuhi.
Dari tabel 6 didapatkan informasi bahwa kedua kondisi tersebut telah dipenuhi. Sehingga dapat diambil kesimpulan bahwa dalam penggunaan kunci publik pada pesan keenam telah memenuhi aturan.

2) Menemukan kepercayaan antar pihak untuk kekinian pesan yaitu penggunaan timestamp.

Notasi yang digunakan yaitu \( P \equiv \#(X) \) dan \( P \equiv \#(\overset{\sim}{X}) \), namun disesuaikan dengan property pada tiap pesan.

Untuk pesan 1 maka notasinya menjadi
\[ S \equiv \{ A \equiv \{ M_2, S \equiv \{ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \} \} \]}

Untuk pesan 2 maka notasinya menjadi
\[ A \equiv \{ S \equiv \{ M_2, A \equiv \{ S \equiv \{ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \} \} \} \]}

Untuk pesan 3 maka notasinya menjadi
\[ S \equiv \{ A \equiv \{ S \equiv \{ A \equiv \{ S \equiv \{ M_2, T_2 \}_K \}_K_{-1} \} \} \]}

Untuk pesan 4 maka notasinya menjadi
\[ A \equiv (M_2), A \equiv S \rightarrow M_2 \]
\[ A \equiv S \equiv M_1 \]
Untuk pesan 5 maka notasinya menjadi
\[ T \equiv \#(M_2), T \equiv A \rightarrow M_2 \]
\[ T \equiv A \equiv M_4 \]
dan
\[ T \equiv \#(M_2), T \equiv A \rightarrow M_5 \]
\[ T \equiv A \equiv M_5 \]
Untuk pesan 6 maka notasinya menjadi
\[ A \equiv \#(M_2), A \equiv T \rightarrow M_5 \]
\[ A \equiv T \equiv M_5 \]

Berikut adalah Tabel 7 yang menunjukkan aplikasi langkah kedua dan langkah ketiga dalam analisis protokol ini.

<table>
<thead>
<tr>
<th>Pesan ke-x</th>
<th>Asumsi (dari langkah kedua)</th>
<th>Logical Formula (dari langkah ketiga)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>[ A \rightarrow S \equiv #(M_2) ]</td>
<td>[ S \equiv A \rightarrow M_2 ]</td>
</tr>
<tr>
<td>2</td>
<td>[ S \rightarrow A \equiv #(M_2) ]</td>
<td>[ A \equiv S \rightarrow M_2 ]</td>
</tr>
<tr>
<td>3</td>
<td>[ A \rightarrow S \equiv #(M_2) ]</td>
<td>[ S \equiv A \rightarrow M_2 ]</td>
</tr>
<tr>
<td>4</td>
<td>[ S \rightarrow A \equiv #(M_2) ]</td>
<td>[ A \equiv S \rightarrow M_2 ]</td>
</tr>
<tr>
<td>5</td>
<td>[ T \rightarrow A \equiv #(M_2) ]</td>
<td>[ S \equiv A \rightarrow M_2 ]</td>
</tr>
<tr>
<td>6</td>
<td>[ S \rightarrow A \equiv #(M_2) ]</td>
<td>[ A \equiv S \rightarrow M_2 ]</td>
</tr>
</tbody>
</table>

Notasi yang akan dipenuhi adalah
\[ A \equiv \#(M_2), A \equiv S \rightarrow M_2 \]
\[ A \equiv S \equiv M_1 \]
Kondisi \[ A \equiv S \equiv M_1 \] akan dipenuhi jika kondisi \[ A \equiv \#(M_2) \] dan \[ A \equiv S \rightarrow M_2 \] dipenuhi.

Dari tabel 7 didapatkan informasi bahwa kedua kondisi tersebut telah dipenuhi. Sehingga dapat diambil kesimpulan bahwa dalam penggunaan timestamp pada pesan kedua telah memenuhi notasi.

**Pesan 3**

Notasi yang akan dipenuhi adalah
\[ S \equiv \#(M_2), S \equiv A \rightarrow M_2 \]
\[ S \equiv A \equiv M_2 \]
Kondisi \[ S \equiv A \equiv M_2 \] akan dipenuhi jika kondisi \[ S \equiv \#(M_2) \] dan \[ S \equiv A \rightarrow M_2 \] dipenuhi.

Dari tabel 7 didapatkan informasi bahwa kedua kondisi tersebut telah dipenuhi. Sehingga dapat diambil kesimpulan bahwa dalam penggunaan timestamp pada pesan ketiga telah memenuhi aturan.

**Pesan 4**

Notasi yang akan dipenuhi adalah
\[ A \equiv \#(M_2), A \equiv S \rightarrow M_2 \]
\[ A \equiv S \equiv M_2 \]
Kondisi \[ A \equiv S \equiv M_2 \] akan dipenuhi jika kondisi \[ A \equiv \#(M_2) \] dan \[ A \equiv S \rightarrow M_2 \] dipenuhi.

Dari tabel 7 didapatkan informasi bahwa kedua kondisi tersebut telah dipenuhi. Sehingga dapat diambil kesimpulan bahwa dalam penggunaan timestamp pada pesan keempat telah memenuhi aturan.

**Pesan 5**

Notasi yang akan dipenuhi adalah
\[ T \equiv \#(M_2), T \equiv A \rightarrow M_2 \]
\[ T \equiv A \equiv M_4 \]
dan
\[ T \equiv \#(M_2), T \equiv A \rightarrow M_5 \]
\[ T \equiv A \equiv M_5 \]
Kondisi \[ T \equiv A \equiv M_5 \] akan dipenuhi jika kondisi \[ T \equiv \#(M_2) \] dan \[ T \equiv A \rightarrow M_5 \] dipenuhi. Dan juga
kondisi \( T \equiv A \equiv M_2 \) akan dipenuhi jika kondisi \( T \equiv\#(M_2) \) dan \( T \equiv A \bowtie M_2 \) dipenuhi. Dari tabel 7 didapatkan informasi bahwa kedua kondisi \( T \equiv\#(M_2) \) dan \( T \equiv\#(M_3) \) tidak dipenuhi. Hal ini disebabkan pada pesan kelima timestamp yang digunakan telah mengalami fungsi hashing, agar kondisi \( T \equiv\#(M_2) \) dan \( T \equiv\#(M_3) \) dipenuhi seharusnya penggunaan timestamp menjadi property independen yang murni dan tidak digabungkan ataupun mengalami proses lain. Sehingga dapat diambil kesimpulan bahwa dalam penggunaan timestamp pada pesan kelima belum memenuhi memenuhi aturan.

**Pesan 6**

Notasi yang akan dipenuhi adalah

\[ A \equiv\#(M_3), A \equiv T \bowtie M_2 \]

Kondisi \( A \equiv T \equiv M_2 \) akan dipenuhi jika kondisi \( A \equiv\#(M_2) \) dan \( A \equiv\#(M_3) \) dipenuhi. Dari tabel 7 didapatkan informasi bahwa kedua kondisi \( A \equiv\#(M_2) \) tidak dipenuhi. Hal ini disebabkan pada pesan kelima timestamp yang digunakan telah mengalami fungsi hashing, agar kondisi \( A \equiv\#(M_2) \) dipenuhi seharusnya penggunaan timestamp menjadi property independen yang murni dan tidak digabungkan ataupun mengalami proses lain. Sehingga dapat diambil kesimpulan bahwa dalam penggunaan timestamp pada pesan keenam belum memenuhi memenuhi aturan.

3) Menemukan kepercayaan antar pihak dalam penggunaan fungsi hash antara Tempat Pemungutan Suara (TPS) dan Server Tabulasi.

Notasi yang digunakan adalah

\[ P \equiv X \Rightarrow H(X) \equiv X \]

Namun disesuaikan dengan properti yang ada pada pesan kelima dan keenam. Sehingga notas untuk pesan kelima adalah \( T \equiv A \bowtie H(M_2) \), \( T < M_2 \)

\[ T \equiv A \bowtie M_2 \]

dan pesan keenam adalah \( A \equiv T \bowtie H(M_3) \), \( A < M_3 \)

\[ A \equiv T \bowtie M_3 \]

**Pesan 5**

Notasi yang akan dipenuhi adalah \( T \equiv A \bowtie H(M_2) \), \( T < M_3 \). Untuk analisis penggunaan fungsi hash, pada langkah kedua tidak digunakan asumsi, karena asumsi digunakan untuk penggunaan kunci publik dan timestamp. Untuk memenuhi kondisi \( T \equiv A \bowtie H(M_2) \) maka dilakukan dengan menggunakan informasi hasil analisis penggunaan kunci publik. Kondisi \( T \equiv A \bowtie\{M_3, M_3, H(T_{anak}[M_2])\}K_a^{-1} \)

dari Tabel 6 atau dapat dituliskan \( T \bowtie M_2 \). Sehingga kondisi \( T \equiv A \bowtie M_3 \) dapat dipenuhi karena kondisi pertama dan kedua telah dipenuhi.

**Pesan 6**

Notasi yang akan dipenuhi adalah \( A \equiv T \bowtie H(M_3) \), \( A < M_2 \). Untuk analisis penggunaan fungsi hash, pada langkah kedua tidak digunakan asumsi, karena asumsi digunakan untuk penggunaan kunci publik dan timestamp. Untuk memenuhi kondisi \( A \equiv T \bowtie H(M_2) \) maka dilakukan dengan menggunakan informasi hasil analisis penggunaan kunci publik. Kondisi \( A \equiv T \bowtie H(T_{sus})[M_2] \) telah dipenuhi sehingga dapat dituliskan \( A \equiv T \bowtie H(M_2) \) telah pula dipenuhi. Kondisi kedua \( A < M_3 \) belum karena \( T \) tidak mengirimkan \( M_3 \) kepada \( A \). \( T \) hanya mengirimkan \( H(T_{sus}[M_3]) \) kepada \( A \). Sehingga penggunaan fungsi hash pada pesan keenam ini belum memenuhi aturan.

**KESIMPULAN**

Dari analisis yang telah dilakukan dengan menggunakan pendekatan BAN Logic, maka dapat disimpulkan bahwa:

1. Penggunaan kunci publik pada protokol
CryptO-0N2 dengan The Blind Schnorr Signature Scheme pendaftaran pesan sampai keenam telah memenuhi peraturan atau notasi yang telah ditentukan.
2. Penggunaan timestamp pada protokol CryptO-0N2 dengan The Blind Schnorr Signature Scheme pendaftaran pesan sampai keenam telah memenuhi peraturan atau notasi yang telah ditentukan sedangkan pada pesan kelima dan keenam belum memenuhi peraturan.
3. Penggunaan fungsi hash pada protokol CryptO-0N2 dengan The Blind Schnorr Signature Scheme pendaftaran pesan kelima telah memenuhi peraturan atau notasi yang telah ditentukan sedangkan pada pesan keenam belum memenuhi peraturan.

Pesan – pesan yang telah memenuhi peraturan untuk penggunaan kunci publik, timestamp, dan fungsi hash berarti pihak yang berkomunikasi pada protocol tersebut telah saling percaya terhadap properti yang dipertukarkan, sedangkan untuk pesan – pesan yang belum memenuhi peraturan maka terdapat kekurangan dalam protokol tersebut yang dapat menghilangkan kepercayaan antar pihak dalam protokol.

Saran untuk penelitian berikutnya adalah melakukan perbaikan terhadap pesan – pesan yang belum memenuhi peraturan dalam penggunaan timestamp dan fungsi hash.

DAFTAR PUSTAKA


LAMPIRAN
A. RINCIAN PROTOTOKOL “CryptO-0N2 with The Blind Schnorr Signature Scheme Implementation”

Berikut adalah rincian protokol tersebut:

1. Tempat pemilihan akan mengirimkan identitas pemilih, identification Number, dan timestamp ke sever penandatagan. Ketiga properti ini kemudian akan ditandatangi menggunakan kunci privat dari tempat pemilihan kemudian selanjutnya dienkripsi menggunakan kunci publik server penandatangan.

\([\{id, iNum, T_2\}K_2^{-1}]K_2\)


Parameter tersebut adalah \(p, q, K\) untuk menghitung \(r\), dengan formulasi \(r = g^K \mod p\). Selanjutnya server akan mengirimkan pesan kepada tempat pemilihan yang berisi identitas pemilih, dan timestamp+1 dan parameter yang telah dibangkitkan. Pesan ini akan ditandatangani oleh server dengan menggunakan kunci privatnya, kemudian akan dienkripsi dengan menggunakan kunci publik tempat pemilihan.

\([\{id, T_{a+1}, p, q, g, r\}K_a^{-1}]K_a\)

3. Setelah menerima pesan dari server, pertama kali tempat pemilihan akan mendekripsinya dengan menggunakan kunci privatnya. Kemudian pesan hasil dekripsi tersebut diverifikasi dengan cara dienkripsi dengan menggunakan kunci publik server. Proses ini akan memverifikasi bahwa benar pesan ini berasal dari server. Selanjutnya properti tersebut telah didapatkan. Hal ini mengindikasikan bahwa pemilih telah dapat melakukan pemilihan. Parameter \(p, q, g, r, K_a\) akan digunakan dalam proses pembuatan (blinding). Selanjutnya tempat pemilihan akan membutakkan pesan hasil pemilihan, \(m\), dengan langkah-langkah:

- Menilai nilai \(\alpha, \beta \in \mathbb{Z}_p\), nilai \((\alpha, \beta)\) dijaga tetap rahasia oleh tempat pemilihan;
- Blinding nilai \(n\) dengan menghitung \(r' = rg^{-\alpha}y^{-\beta} \mod p\);
- Hitung nilai \(e' = H(m, r')\);
- Hitung nilai \(e = e' + \beta \mod q\);

Kirim nilai \(e\) server penandatanganan.

Kedua pesan ini akan ditandatangani menggunakan kunci privat dari tempat pemilihan kemudian selanjutnya dienkripsi menggunakan kunci publik server penandatanganan.

\([\{e, T_a+2\}K_a^{-1}]K_a\)

Selanjutnya signor menghitung $s$, dengan formulasi:

$$g^s y^s = r \mod p$$

Selanjutnya server akan mengirimkan $s$ ke tempat pemilihan. Pesan ini akan ditandatangani oleh server dengan menggunakan kunci privatnya, kemudian akan dienkripsi dengan menggunakan kunci publik tempat pemilihan.

$$\left\{ s, T_{a+4} \right\}_K_e^{-1} K_a$$

5. Setelah menerima pesan dari server, pertama kali tempat pemilihan akan mendekripsinya dengan menggunakan kunci privatnya. Kemudian pesan hasil dekripsi tersebut diverifikasi dengan cara didekripsi dengan menggunakan kunci publik server. Proses ini akan memverifikasi bahwa benar pesan ini berasal dari server. Selanjutnya $s$ yang telah didapatkan akan dihitung untuk mendapatkan tanda tangan digital yang berkorespendensi dengan $m$ (pilihan), dengan langkah:

Hitung:

$$s' = s - x \mod q$$

Pasangan $(e', s')$ adalah Schnorr sign dari pesan $m$.

Sehingga tempat pemilihan telah mendapatkan tanda tangan digital yang berkorespendensi dengan pesan $m$, yaitu pasangan $(e', s')$.

Selanjutnya untuk proses pemilihan, tempat pemilihan akan mengirimkan pilihan dan tanda tangan digital yang berkorespendensi untuk diverifikasi oleh server perhitungan suara.

Setelah mendapatkan pesan dan tanda tangan digital yang berkorespendensi maka properti ini akan dikirimkan ke server perhitungan suara untuk validasi dan dihitung pilihannya.

Tempat pemilihan akan mengirimkan pilihan pesan dan tanda tangan digital yang berkorespendensi dengan pilihan tersebut yaitu $(m, e', s')$.

Selain itu tempat pemilihan akan mengirimkan $r'$ kepada server tabulasi suara untuk proses verifikasi.

Untuk fungsi freshness ditambahkan pula fungsi timestamp yaitu $T_{a+4}$. Untuk mencegah reverse terhadap timestamp, maka timestamp ini akan menjadi input suatu fungsi hash. Selain itu timestamp akan digabung dengan $r'$.

Kelima properti ini kemudian akan ditandatangani menggunakan kunci privat dari tempat pemilihan kemudian selanjutnya dienkripsi menggunakan kunci publik server perhitungan suara.

$$\left\{ \left\{ m, r', e', s', H(T_{a+4} || r') \right\}_K_e^{-1} \right\}_K_a$$


Kemudian server tabulasi suara akan menghitung nilai hash dari $T_{a+4}$ digabung dengan $r'$. Jika nilainya sama dengan nilai $H(T_{a+4} || r')$ yang tempat pemilihan kirimkan maka benar pesan tersebut fresh.

Kemudian server akan menghitung $H(m, r')$ dan $H(\{ m, g^s y^s \mod p \}$.

Jika kedua nilai yang dihitung sama maka pesan dan tanda tangan digital yang berkorespendensi dinyatakan valid.

Selanjutnya pilihan dapat dimasukkan untuk tabulasi suara.

Untuk mengakhiri protokol ini maka server tabulasi suara akan mengirimkan properti berikut:

$$\left\{ \left\{ H(T_{a+4} || r') \right\}_K_e^{-1} \right\}_K_a$$


Selanjutnya tempat pemilihan akan menghitung nilai hash dengan input $T_{a+5}$ dan $r'$. Nilai tersebut akan dibandingkan dengan nilai $H(T_{a+5} || r')$ yang dikirimkan oleh server tabulasi. Jika nilainya sama maka pesan ini adalah fresh.
DISKUSI

Pertanyaan : Ciri – cirri apa yang membedakan model dari ketiga distribus tersebut?
Jawab : dapat dilihat dari ekor pada gambaran hasil

Pertanyaan : Apa makna dari ekor pendek gamma dan ekor panjang gamma?
Jawab : berkaitan dengan sebaran data