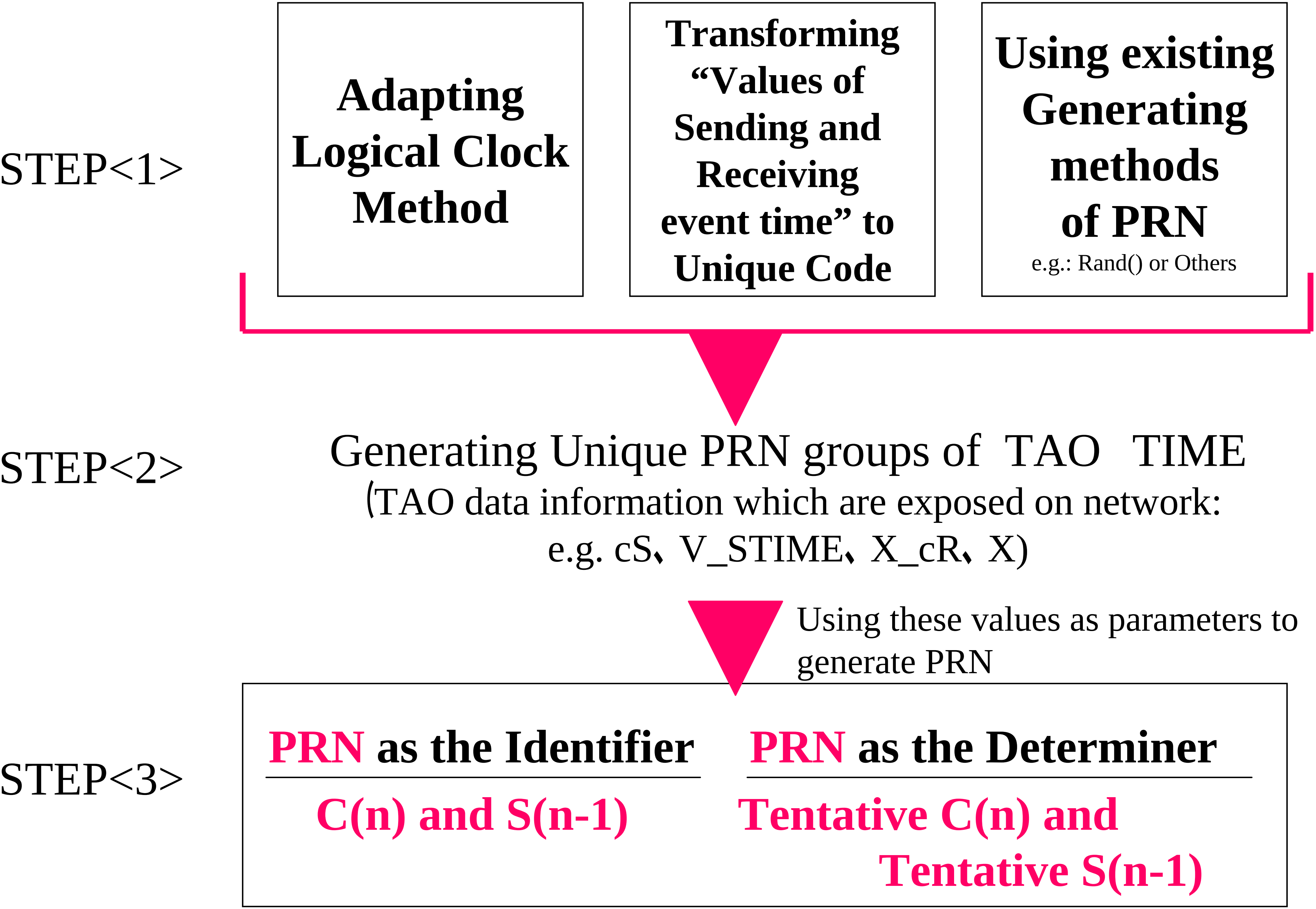
Presentation material
for
Lamp Session
on
CRYPTREC Workshop

JCN Co., Ltd.

Jan. 28th, 2002

Procedures to generate PRN in TAO TIME Cognition Algorithm



STEP<1>

Adapting Logical Clock Method

Transforming "Values of Sending and Receiving event time" to Unique Code

Using existing Generating methods of PRN

e.g.: Rand() or Others

STEP<2>

Generating Unique PRN groups of TAO TIME

（TAO data information which are exposed on network:
e.g. cS、V_STIME、X_cR、X)

Using these values as parameters to generate PRN

STEP<3>

PRN as the Identifier

C(n) and S(n-1)

PRN as the Determiner

Tentative C(n) and Tentative S(n-1)

Generating methods of
C(n) , S(n-1) , Tentative C(n) and Tentative S(n-1)

Client Identifier・・・・・To be generated at Client and to be sent to Server.

$$C(n) = S(n-1) - \{cS(n-1) - cR(n-2)\}$$

***Nobody knows the values of S(n-1), cS(n-1) and cR(n-2) except proper Client. The only way to get these value is to conjecture with conjecturing a(n-1) , X(n-2) and/or a(n-2) which are generated by Rand().**

Client Determiner・・To be generated at Server, and to be collated with C(n) to execute cognition.

$$\text{Tentative } C(n) = < C(n-1) + \{ sR(n-1) - sR(n-2) \} > - \{cS(n-1) - cR(n-2)\}$$

- **There is no table to generate a() at the Server. In addition to this, Seed value changes at each access, and Seed value will not be shared between Server and clients.**

Server Identifier： To be generated at Server and to be sent to Client.

$$S(n-1) = C(n-1) + \{sR(n-1) - sR(n-2)\}$$

Server Determiner ： To be generated at Client, and to be collated with S(n-1) to execute cognition.

$$\text{Tentative } S(n-1) = C(n) + \{ cS(n-1) - cR(n-2) \}$$

Our Requests to Evaluation Committee of CRYPTREC

1. Reconsideration the object to evaluate.

   - In the procedure of evaluation you have done, you have set the point aimed at a(n), it's the out of our design.
     We eagerly request you to reconsider the object to evaluate not a(n) but C(n), S(n-1), Tentative C(n) and Tentative S(n-1) with following reasons;-

   <The reason 1>

   - The values of a(n-2) and a(n-1) are the mandatory data to generate Tentative C(n) and Tentative S(n-1) at the Server,
   - To calculate a(n-2) and a(n-1), Server ought to get the values of cS(n-2), cR(n-2), cS(n-1) and cR(n-1) which were generated at the client in last 2 generations of access transmissions, with the Client's permission

   <The reason 2>

   - There is no encrypt table and Seed value to generate a( ) at the Server.

2. **We would like you to put rational evidence when you describe such as "It's seems to have problem in security".**