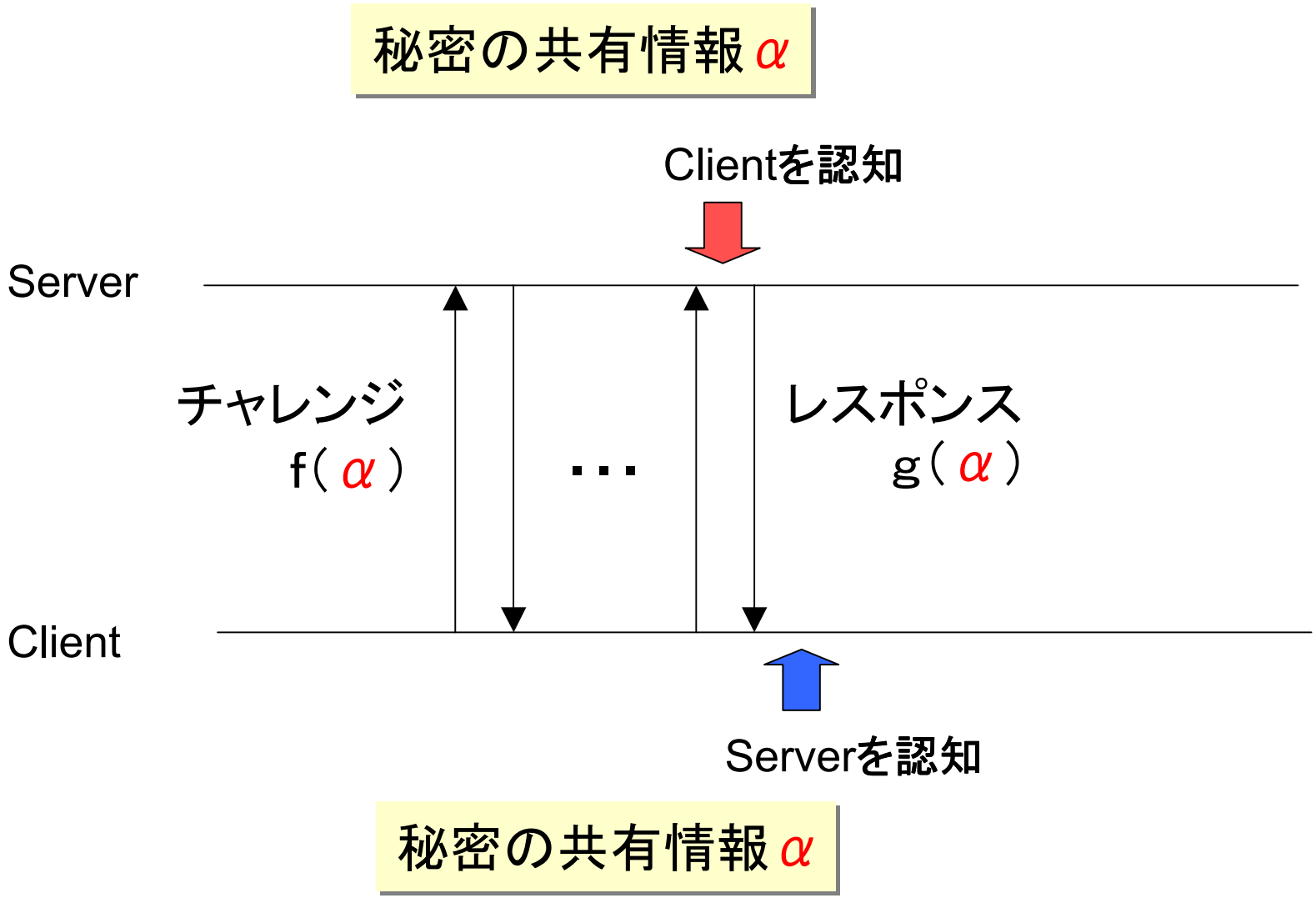
TAO TIME暗号評価の現状報告
(スクリーニング評価)

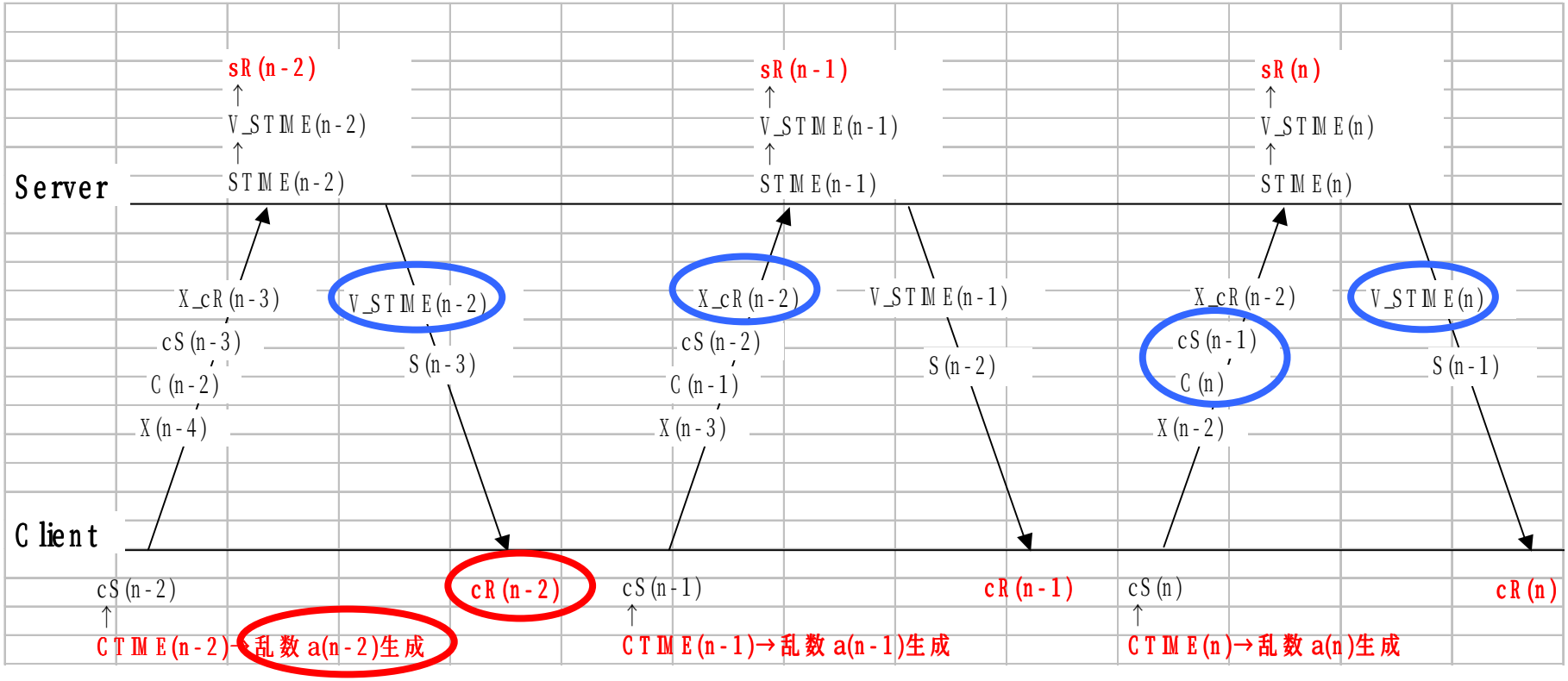
平成14年1月28日

共通鍵暗号評価小委員会
委員　宝木　和夫

TAO　TIMEにおける相手認証基本フロー



処理シーケンスイメージ



$$cR(n-2) = \langle V\_STIME(n-2) \ldots + \{cR(n-3) - cS(n-3)\} + \ldots + a(n-2) \rangle + 1$$

$$X\_cR(\mathbf{n-2}) = cR(\mathbf{n-2}) + \{\alpha(X(\mathbf{n-2})) + \beta(X(\mathbf{n-2}))\}$$

－－－－－赤字はネットワークに露出しないTAOデータ情報－－－

評価対象とした擬似乱数生成関数

CRYPTRECとしての着目点

乱数a (n)が今回募集の擬似乱数生成関数か
→他に見当たらないのでそのように評価
→a (n)は擬似乱数生成関数として認められるか

評価対象となるa (n)の計算式：

【CTIME(n)の計算式】：CTIME(n) ＝クライアント・ローカルクロックの送信イベント時（現在時刻のミリ秒）

【rand()の初期値計算式】：a (n-1) ＊1000 ＋CTIME(n) mod 1000
上記計算は、a (n-1)を生成する毎に毎回行う。

a (n)＝a (n-1)＋{rand( )+1}＊100000 ＋CTIME(n) mod 100000

ANSI 規格C 言語によるrand関数について

- rand関数は0 と RAND_MAX の間のランダムな整数を発生させる
- ANSI C の規格で決められていることは RAND_MAX は最低 32767 なければならないことのみ
- ANSI の規格に準拠した C 言語であっても、計算法などは違っていてもよい
- しかし、実際のところ、rand() で生成される疑似乱数は線型合同法によるもののみのよう

実例として Visual C++ の場合を見れば、

$x_1 = 1$　　(これが seed。srand() で変更可)

$x_n \equiv 214013 * x_{n-1} + 2531011 \bmod 2^{31}$

$X = (x_n/2^{16})$ の整数部分　$(0 < X < 2^{15})$

a(n)系列について

● CTIME(n)は現在時刻（送信時）のミリ秒表示をしたもの。
つまり、物理タイム

● 計算式
a (n)＝a (n-1)＋{rand( )+1}＊100000 ＋CTIME(n) mod 100000

より、a (n)－a (n-1)を10進表記したときの下5桁は
CTIME(n)10進表記の下5桁と一致する

つまり、a (n)－a (n-1)の下5桁が常に物理タイムとなる

評価者1の評価

結論：詳細評価を行う必要はない

コメント（抜粋）：

● 仕様書では、クライアント、サーバー間の簡単な認証機能を供給することを主な目的として記述されている。

● マイナーな改良を施すことにより、疑似乱数を生成する仕様に変更することは可能である。

● しかし、本仕様では暗号学的な関数（公開鍵暗号で基本的に用いられる演算（素体や、拡大体、それに準じる環、群での加算、乗算など）、ハッシュ関数、疑似乱数生成器（鍵ストリーム生成器）、ブロック暗号）をまったく用いておらず、どのような改良を加えたところで安全な鍵生成などに用いる乱数生成は期待できない。

評価者2の評価

結論：詳細評価を行う必要はない

コメント（抜粋）：

● 暗号技術仕様書の「1.はじめに」の中で応募者は、「TAO TIME 認知アルゴリズムはネットワーク上の任意の2 地点に存在する client と server 間の相互認知システム構築を目的とする認知アルゴリズムである」と主張しており仕様書にはその認知アルゴリズムが記述されている。

● この暗号技術仕様書は疑似乱数生成器の仕様書に必要な「種(入力値)に対して(疑似乱)数列を出力する決定的アルゴリズム」を記述したものではないと判断した。

● したがって応募書類の不備としてスクリーニング評価対象とは認められず詳細評価を行う必要はないとの結論に至った。

評価者3の評価

結論：詳細評価を行う必要はない

コメント（抜粋）：

● 乱数生成技術として応募されているが、乱数生成を利用した“認知”システムの提案であり、乱数生成は既存の方法を利用しているに過ぎない。また、“認知”システムとしてみても、説明が不十分である上に安全性にも問題があるように思える。

● 乱数を導入することが“認知”のために重要と思われるがそれに関して説明されていない。

評価者4の評価

結論：詳細評価を行う必要はない

コメント（抜粋）：

● 提案者がTAO TIME 認知アルゴリズムが擬似乱数生成系であると主張する根拠が全く認められない。評価者は、本方式が擬似乱数生成系ではないと判断する。よって詳細評価を行う必要はない。

● 提案者がTAO TIME 認知アルゴリズムが擬似乱数生成系であると主張する根拠がない。もし提案者がそう主張するのであれば、生成された擬似乱数列の周期、線形複雑度、0/1 等頻度性などに関する評価をしなければならない。

CRYPTREC共通鍵暗号評価委員会としての評価

見解：詳細評価を行う必要はない

理由：

● 乱数生成技術として応募されているが、乱数生成を利用した“認知”システムの提案となっている。

● マイナーな改良を施すことにより、乱数生成技術としての応募仕様に変更することは可能である。

● しかし、提案者がTAO TIME 認知アルゴリズムが擬似乱数生成系であると主張する根拠に乏しい、と判断される。