

# Верификация криптографических протоколов на основе понятия наблюдаемой эквивалентности

А. М. Миронов (МГУ им. М. В. Ломоносова, Москва)

В работе излагается модель криптографических протоколов, основанная на теории процессов с передачей сообщений. Показано, как можно использовать данную модель для решения задач верификации криптографических протоколов (то есть построения математических доказательств утверждений о том, что криптографические протоколы обладают заданными свойствами). В качестве примера таких свойств рассматриваются свойства целостности и секретности. Данные свойства определяются формально, как некоторые соотношения, выражаемые в терминах наблюдаемой эквивалентности процессов с передачей сообщений. Показаны примеры верификации данных свойств для некоторых криптографических протоколов.

**Ключевые слова:** криптографические протоколы, верификация, наблюдаемая эквивалентность.

## 1. Процессная модель криптопротоколов

**Криптографический протокол (КП)** — это распределённый алгоритм, определяющий порядок обмена сообщениями между несколькими агентами. Сообщения, передаваемые в процессе работы КП, могут иметь зашифрованный вид. В излагаемой ниже процессной модели КП и их формальные спецификации представляются в виде графов, ребра которых помечены **операторами**. Операторы представляют собой выражения, состоящие из термов и формул.

Множество  $\mathcal{E}$  **термов** определяется индуктивно: переменные и константы являются термами, если  $e_1, \dots, e_n$  — список термов, то запись  $(e_1, \dots, e_n)$  является термом, и для каждого ключа  $k$  и каждого терма  $e$  запись  $k(e)$  является термом. Если  $e_1 = e'_1, \dots, e_n = e'_n$  — список равенств термов (который может быть пустым), то запись

$$\llbracket e_1 = e'_1, \dots, e_n = e'_n \rrbracket$$

называется **формулой**.

**Подстановкой** называется запись  $\theta$  вида  $e'/e$ , где  $e, e' \in \mathcal{E}$ .

**Действие** — это конструкция  $a$  одного из трёх перечисляемых ниже видов. Каждой паре  $(a, \xi)$ , где  $a$  — действие, и  $\xi$  — означивание переменных, входящих в  $a$ , соответствует **выполнение**  $a^\xi$  действия  $a$  на означивании  $\xi$ , неформально определяемое ниже.

- 1) **Ввод** — это действие вида  $e_1?e_2$ , где  $e_1, e_2 \in \mathcal{E}$ . Выполнение  $(e_1?e_2)^\xi$  заключается в получении сообщения через канал  $e_1^\xi$ , и записи значений, соответствующих компонентам полученного сообщения, в переменные, входящие в терм  $e_2$ .
- 2) **Вывод** — это действие вида  $e_1!e_2$ , где  $e_1, e_2 \in \mathcal{E}$ . Выполнение  $(e_1!e_2)^\xi$  заключается в посылке сообщения  $e_2^\xi$  через канал  $e_1^\xi$ .
- 3) **Внутреннее действие** — это действие вида  $b\theta$ , где  $b$  — формула, и  $\theta$  — подстановка. Выполнение  $(b\theta)^\xi$  возможно только если  $b^\xi = 1$ , и заключается в изменении  $\forall i = 1, \dots, n$  значения переменной  $x_i$ : новое значение  $x_i$  полагается равным  $e_i^\xi$ .

**Процесс с передачей сообщений** (называемый ниже просто **процессом**) — это пятёрка  $P = (S, s^0, R, b, X^-)$ , компоненты которой имеют следующий смысл:  $S$  — множество **состояний** процесса  $P$ ;  $s^0 \in S$  — **начальное состояние** процесса  $P$ ;  $R \subseteq S \times \mathcal{A} \times S$  — множество **переходов** процесса  $P$  (где  $\mathcal{A}$  — множество действий);  $b$  — формула, называемая **предусловием** процесса  $P$ ;  $X^-$  — множество переменных, называемых **скрытыми переменными** процесса  $P$ . Переход  $(s_1, a, s_2)$  называется **вводом**, **выводом** или **внутренним переходом**, если  $a$  — ввод, вывод или внутреннее действие, соответственно. Процесс  $P = (S, s^0, R, b, X^-)$  можно представлять себе в виде помеченного графа (обозначаемого тем же символом  $P$ ), вершинами которого являются состояния из  $S$ , а рёбрами — переходы из  $R$ : каждому переходу  $(s_1, a, s_2)$  соответствует ребро из  $s_1$  в  $s_2$  с меткой  $a$ , мы будем обозначать данное ребро записью  $s_1 \xrightarrow{a} s_2$ . Каждый сеанс  $\sigma$  **выполнения процесса**  $P$  представляет собой обход графа  $P$  (начиная с начального состояния), с выполнением действий, которые являются метками проходимых рёбер.

## 2. Наблюдаемая эквивалентность

Множество термов  $E \subseteq \mathcal{E}$  называется **замкнутым**, если оно удовлетворяет следующим условиям:

- если  $\forall i = 1, \dots, n \ e_i \in E$ , то  $(e_1, \dots, e_n) \in E$ ,
- если  $E$  содержит терм вида  $(e_1, \dots, e_n)$ , то  $\forall i = 1, \dots, n \ e_i \in E$ ,
- если  $k, e \in E$ , где  $k$  — ключ, то  $k(e) \in E$ ,
- если  $E$  содержит терм вида  $k(e)$ , и  $k \in E$ , то  $e \in E$ .

Замкнутые множества термов используются для представления множеств сообщений, которые могут быть известными противнику. Указанные выше правила соответствуют операциям, которые может выполнять противник с имеющимися у него сообщениями:

- если противник имеет сообщения  $e_1, \dots, e_n$ , то он может скомпоновать из них сообщение  $(e_1, \dots, e_n)$ ,
- если противник имеет сообщение вида  $(e_1, \dots, e_n)$ , то он может получить его составные части  $e_1, \dots, e_n$ ,
- если противник имеет ключ  $k$  и сообщение  $e$ , то он может создать шифртекст  $k(e)$ , и
- если противник имеет шифртекст  $k(e)$  и ключ  $k$ , то он может расшифровать этот шифртекст, то есть получить сообщение  $e$ .

Нетрудно доказать, что  $\forall E \subseteq \mathcal{E}$  существует наименьшее по включению замкнутое множество  $E^\omega \subseteq \mathcal{E}$  (называемое **замыканием** множества  $E$ ), такое, что  $E \subseteq E^\omega$ .

**Полнение** процесса  $P$  — это пара  $(P, \eta)$ , где  $\eta$  — функция, сопоставляющая каждому состоянию  $s$  процесса  $P = (S, s^0, R, b, X^-)$  подмножество  $\eta(s) \subseteq \mathcal{E}$ , причем выполнено следующее условие:  $\eta(s^0)$  содержит все константы и все нескрытые переменные процесса  $P$ , для каждого перехода  $s_1 \xrightarrow{a} s_2$  процесса  $P$   $\eta(s_1) \subseteq \eta(s_2)$ , и если  $a$  имеет вид  $b\theta$ , то  $\forall i = 1, \dots, n$  из  $e_i \in \eta(s_1)^\omega$  следует  $x_i \in \eta(s_2)$ , а если  $a$  имеет вид  $e_1?e_2$  или  $e_1!e_2$ , и  $e_1 \in \eta(s_1)^\omega$ , то  $e_2 \in \eta(s_2)$ .

Полнение  $(P, \eta)$  процесса  $P$  можно интерпретировать как добавление к каждому состоянию  $s$  процесса  $P$  совокупности  $\eta(s)$  тех сообщений, которые процесс  $P$ , находясь в состоянии  $s$ , мог передать другим процессам, или получить от других процессов, и, следовательно, которые могут быть известны противнику.

Ниже мы определяем понятие наблюдаемой эквивалентности двух процессов. Мы будем обозначать записью  $P_1 \approx P_2$  утверждение о том, что процессы  $P_1$  и  $P_2$  находятся в отношении наблюдаемой эквивалентности. Понятие наблюдаемой эквивалентности имеет следующий неформальный смысл: процессы  $P_1$  и  $P_2$  наблюдаемо эквивалентны, если для любого внешнего наблюдателя их поведение неразличимо.

Ниже мы будем использовать следующие понятия и обозначения.

- 1) Пусть задан процесс  $P = (S, s^0, R, b, X^-)$  и пара состояний  $s, s' \in S$ . **Составной переход (СП)** из  $s$  в  $s'$  — это последовательность  $A$  переходов из  $R$  вида

$$s = s_0 \xrightarrow{a_1} s_1, \quad s_1 \xrightarrow{a_2} s_2, \quad \dots \quad s_{n-1} \xrightarrow{a_n} s_n = s'$$

такая что среди  $a_1, \dots, a_n$  не более одного оператора ввода или вывода.

- 2) Если  $b$  и  $b'$  — формулы, то запись  $b \leq b'$  является сокращённой записью утверждения о том, что  $b'$  является логическим следствием  $b$ .

Пусть заданы процессы  $P_i = (S_i, s_i^0, R_i, b_i, X_i^-)$  ( $i = 1, 2$ ), причем  $S_1 \cap S_2 = \emptyset$ . Процессы  $P_1$  и  $P_2$  **наблюдаемо эквивалентны**, если существует совокупность  $\{b_{s_1 s_2} \mid s_i \in S_i (i = 1, 2)\}$  формул, каждая переменная в которых является нескрытой переменной  $P_1$  или  $P_2$ , обладающих следующими свойствами:

- 1)  $b_1 \wedge b_2 \leq b_{s_1^0 s_2^0}$ ;
- 2) для каждого перехода  $s_1 \xrightarrow{a} s'_1$  процесса  $P_1$  и каждого состояния  $s_2 \in S_2$  существует СП  $s_2 \xrightarrow{A} s'_2$  процесса  $P_2$ , такой что

$$b_{s_1 s_2} \wedge \llbracket a \rrbracket \leq (a, A) b_{s'_1 s'_2},$$

где запись  $(a, A) b_{s'_1 s'_2}$  обозначает формулу, определяемую индуктивно следующим образом:

(ниже предполагается, что СП  $A$  имеет вид  $s_2 \xrightarrow{a_1} \dots \xrightarrow{a_{n-1}} s''_2 \xrightarrow{a_n} s'_2$ , и запись  $A \setminus a_n$  обозначает СП  $s_2 \xrightarrow{a_1} \dots \xrightarrow{a_{n-1}} s''_2$ )

- a)  $b \wedge b_{s'_1 s'_2}$ , если  $a = b \Lambda$ , и  $A$  — пустой СП,
- b)  $(b \Lambda, A) \theta(b_{s'_1 s'_2})$ , если  $a = b \theta$ ,
- c)  $(a, A \setminus a_n) (b \wedge \theta(b_{s'_1 s'_2}))$ , если  $a_n = b \theta$ ,



Поведение агентов  $a$  и  $b$  представляется процессами  $A$  и  $B$ , где

$$A \stackrel{\text{def}}{=} \langle c!k(x) \rangle \mathbf{0}, \quad B \stackrel{\text{def}}{=} \langle c?k(y) \rangle P.$$

КП представляется процессом  $Sys \stackrel{\text{def}}{=} (A, B)_k$ .

Формальное описание свойств целостности и секретности этого КП имеет следующий вид.

- 1) Свойство **целостности** данного КП заключается в том, что в результате работы этого КП передаваемое сообщение доходит до получателя в точности в том же виде, в котором оно было послано отправителем.

Свойство целостности выражается соотношением  $Sys \approx \tilde{S}ys$ , где  $\tilde{S}ys \stackrel{\text{def}}{=} (A, \tilde{B})_k$ ,  $\tilde{B} \stackrel{\text{def}}{=} \langle c?k(y) \rangle \langle x/y \rangle P$ . Процесс  $\tilde{S}ys$  описывает КП, отличающийся от исходного КП модификацией агента  $b$ : после того, как этот агент выполнил действия получения сообщения и записи его в  $y$ , в эту переменную заносится сообщение, которое в действительности посылал агент  $a$ , то есть  $x$ .

- 2) Свойство **секретности** КП заключается в том, что для любой пары  $x, x'$  сообщений, каждое из которых  $a$  может передать  $b$  при выполнении этого КП, и для двух сеансов выполнения этого КП, в первом из которых передаётся  $x$ , а во втором —  $x'$ , никакой внешний (то есть отличный от участников  $a, b$  КП) агент, наблюдающий за выполнением этих сеансов, не имеет возможности извлечь из наблюдаемой информации какие-либо знания о том, одинаковы ли сообщения  $x, x'$ , или различны (если только эти знания не разглашаются самими участниками КП).

Свойство секретности данного КП выражается импликацией

$$\langle x/y \rangle P \approx \langle x'/y \rangle P \quad \Rightarrow \quad Sys \approx \langle x'/x \rangle Sys.$$

Формальное обоснование этих соотношений производится на основе определения отношения наблюдаемой эквивалентности процессов.

## Список литературы

- [1] Миронов А. М. Метод доказательства наблюдаемой эквивалентности процессов с передачей сообщений // Информатика и её применения. — 2014. — Т. 8. Вып. 2. — С. 57–71.