Г.В. МАТВЕЕВ, В.В. МАТУЛИС

СОВЕРШЕННАЯ ВЕРИФИКАЦИЯ МОДУЛЯРНОЙ СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА

Белорусский государственный университет, Минск, Беларусь

matveev@bsu.by, uladzislau.matulis@yandex.by

Схемы разделения секрета используются для распределения секретного значения среди группы пользователей таким образом, что только разрешенные подмножества пользователей могут правильно восстановить секрет. Изучаемая нами модулярная схема разделения секрета (МСРС) основывается на китайской теореме об остатках. В этой схеме секреты $s(x)$, $S(x)$, $s_1(x)$,…, $s_k(x)$ определяются следующим образом: $s(x) = S(x) \bmod m(x)$, $s_i(x) = S(x) \bmod m_i(x)$, i=1, …, k. Все секреты $s(x)$, $S(x)$, $s_1(x)$, …, $s_k(x)$ и модули $m(x)$, $m_1(x)$, …, $m_k(x)$ являются элементами кольца полиномов $F_p[x]$, а восстановление секрета $s(x)$ осуществляется путем применения упомянутой китайской теоремы об остатках. Под верификацией любой схемы разделения секрета понимают протокол проверки участниками их частичных секретов и (или) протокол проверки законности действий дилера. В своем докладе мы предлагаем способы совершенной верификации МСРС. Это означает, что в результате верификации никто из участников и неразрешенные подмножества участников не получают никакой информации о секрете $s(x)$, кроме априорной. В работе предложены два способа верификации. Первый способ – более простой; он основан на предположении о честности дилера. Если дилер нечестный, то верификация является более сложной. Оба способа основываются на одной работе Дж. Бенало и обобщают протокол предложенный ранее М. Васьковским и Г. Матвеевым в двух направлениях. Во-первых, верифицируется общая, а не только пороговая структура доступа, а во-вторых, дилер не обязательно честный. Ранее Н. Шенец нашел условие совершенности МСРС. Таким образом, при соблюдении этого условия совершенными являются и МСРС и протокол ее верификации.