ПОРОГОВАЯ СХЕМА РАЗДЕЛЕНИЯ СЕКРЕТОВ С ИСПОЛЬЗОВАНИЕМ ПОЛИНОМИАЛЬНОГО КОДА

Калмыков И.А., Науменко Д.О., Березкина М.В., Макарова А.В.,

Калмыков М.И.

Северо-Кавказский федеральный университет

Институт информационных технологий и телекоммуникаций

г. Ставрополь, Россия

Постановка задачи. Особо актуальны вопросы реализации информационной безопасности при построении беспроводных самоорганизующихся сетей (ad hoc сетей), которые представляют собой децентрализованные не имеющие постоянной структуры динамические сети. Такие сети характеризуются быстрым развертыванием при минимальной конфигурировании, что позволяет эффективно применять их в чрезвычайных ситуациях, таких как катастрофы и военные конфликты.

Однако самоорганизующиеся сети характеризуются незащищённость узлов от злоумышленника, который легко может получить один в распоряжение. Поэтому разработка схемы разделения секретов, позволяющей не только восстановить ключ для группы пользователей, но и обнаружить факт навязывания ложного образа, является актуальной.

Решение задачи. В настоящее время известно несколько методов разделения секретов, позволяющих решить эту задачу [1]. Особое место среди них занимает схема разделения секретов на основе полиномиальной системы классов вычетов (ПСКВ). В данной схеме используются неприводимые полиномы $p_i(z)$. Для реализации (t, n)-поро-говой схемы разделения секрета выбирается полином $p_x(z)$, такой что

$$deg\ p_x(z) > deg\ M(z), \quad (1)$$

где M(z) - полиномиальную форму секрета.

Затем выбираются система упорядоченных неприводимых полиномов $p_i(z)$, удовлетворяющих условию

$$deg\ p_1(z) \le deg\ p_2(z) \le \ldots \le deg\ p_n(z), \quad (2)$$

где $deg\ p_i(z) \le deg\ p_x(z)$; i=1, 2, …, n.

Для (t, n)-пороговой схемы проверяется выполнение условия

$$deg(p_1(z)p_2(z)\ldots p_t(z)) > deg(p_x(z)p_{n-t+2}(z)p_{n-t+3}(z)\ldots p_n(z)). \quad (3)$$

Чтобы определить доли секрета и их распределить между абонентами группы, выбирается полином r(z) и вычисляется значение

$$M^*(z) = M(z) + r(z)p_x(z). \quad (4)$$

В качестве долей для каждого пользователя выступают остатки

$$M_i^*(z) \equiv M(z) mod\ p_i(z). \quad (5)$$

Используя китайскую теорему об остатках, t пользователей способны восстановить M*(z), а затем, зная r(z) и $p_x(z)$, определить M(z).

Пример. Пусть в качестве полинома выбрали $p_x(z)=z^4+z+1$. Значение секрета равно $M(z)=z^3$. Необходимо построить (3,4)-пороговую схему, функционирующую в ПСКВ.

Выбираем систему полиномов $p_1(z)=z+1$, $p_2(z)=z^2+z+1$, $p_3(z)=z^4+z^3+z^2+z+1$, $p_4(z)=z^4+z^3+1$. Вычислим рабочий диапазон $P_t(z)=\prod_{i=1}^{3} p_i(z)=z^7+z^6+z^5+z^2+z+1$. Пусть $r(z)=z^6$.

Для определения M*(z) воспользуемся выражением (4). Тогда $M^*(z)=(z^3+z^6(z^4+z+1)) \bmod P_t(z)=z^6+z^5+z^3+z^2$.

Доли секрета $M_1^*(z)=M^* \bmod p_1(z)=0$, $M_2^*(z)=M^* \bmod p_2(z)=0$, $M_3^*(z)=M^* \bmod p_3(z)=z^3+z^2+z+1$, $M_4^*(z)=M^* \bmod p_4(z)=z^3$.

В восстановлении секрета M(z) участвуют 1, 2 и 4 абоненты. Они обмениваются $M_1^*(z), p_1(z)$; $M_3^*(z), p_3(z)$; $M_4^*(z), p_4(z)$ и вычисляют базисы $B_1(z)=z^8+z^4+z^2+z+1$, $B_3(z)=z^6+z^5+z^4+z^3+z^2+1$, $B_4(z)=z^8+z^6+z^5+z^3+z+1$. Затем, определив значение диапазона $P_{134}(z)=\prod_{i=1,3,4} p_i(z)=z^9+z^8+z^5+z^4+z^3+1$, используют китайскую теорему об остатках для восстановления образа M*(z). Тогда имеем

$$M^*(z)=\sum_{i=1,3,4} M_i^*(z)B_i(z) \bmod P_{134}(z)=z^6+z^5+z^3+z^2.$$

Зная значение $r(z)=z^6$ и применяя (4), получаем секрет $M(z)=z^3$.

Применение ПСКВ позволяет также обнаруживать ложный образ, навязываемый противником. Если в данную систему оснований добавить проверочный модуль $p_{n+1}(z)$ такой, что

$$deg(p_{n+1}(z)) \geq deg(p_n(z)), \qquad (6)$$

то схема разделения в ПСКВ отыщет и устранит ложный образ.

Для выполнения данной процедуры можно воспользоваться методом проекций. Проекцией полинома A(z) по основанию pj(z) называется полином Aj(z), полученный путем вычеркивания остатка по основанию pj(z). Если образ секрета M*(z) не содержит ложного образа, то все проекции по основаниям будут принадлежать рабочему диапазону. Если в коде ПСКВ есть ложный образ, то все проекции будут выходить за приделы рабочего диапазона, за исключением ошибочного образа.

Воспользуемся основаниями примера, представленного выше. В качестве контрольного модуля - $p_5(z)=z^4+z+1$. Пусть образ секрета M*(z)=z6 принадлежит рабочему диапазону Рраб(z)=z7+z6+z5+z2+z+1 и в модулярном коде имеет вид M*(z)=(1, 1, z, z3+z2+z+1, z3+z2). Пусть противник узнал значение основания p3(z) и навязывает образ $\alpha_3^{лож}(z)=1$. Проведем проекцию M*(z)=(1, 1, 1, z3+z2+z+1, z3+z2).

Удалим остаток $\alpha_1(z)=1$. Тогда M*(z)=(1, 1, z3+z2+z+1, z3+z2). В полученной системе с основаниями p2(z)=z2+z+1, p3(z)=z4+z3+z2+z+1, p4(z)=z4+z3+1, p5(z)=z4+z+1 диапазон P1(z)=z14+z13+z12+z10+z9+z8+z7+z6 +z5+z4+z3+z2+z+1.

Ортогональные базисы равны
B21(z)=z12+z9+z6+z3+1
B31(z)=z10+z5+1;
B41(z)=z10+z8+z5+z4+z3+z+1;
B51(z)=z12+z9+z8+z6+z4+ z3+z2+z.
Тогда

$$M_1^* = \left|1B_2^1(z)+1B_3^1(z)+(z^3+z^2+z+)B_4^1(z)+(z^3+z^2)B_5^1(z)\right|_{P^1(z)}^{+} =$$

$$= z^{10}+z^9+z^5+z+1; \quad deg\, M_1^*(z) > deg\, P_{раб}(z)$$

Следовательно, остаток $\alpha_1(z)=1$ не является ложным.

Удалим остаток $\alpha_2(z)=1$. Тогда M*(z)=(1, 1, z3+z2+z+1, z3+z2). В полученной системе с основаниями p1(z)=z+1, p3(z)=z4+z3+z2+z+1, p4(z)=z4+z3+1, p5(z)=z4+z+1 диапазон P2(z)=z13+z12+z10+z9+z8+z6+z4 +z3+z+1. Ортогональные базисы равны
B12(z)=z12+z9+z6+z3+1 ;
B32(z)= =z12+z10+z9+z6+z5+z3;
B42(z)=z12+z10+z9+z8+z6+z5+z4+z3+z2+1;
B52(z)=z12+z9+z8+z6+z4+z3+z2+z;
Тогда

$$M_2^* = \left|1B_1^2(z)+1B_3^2(z)+(z^3+z^2+z+)B_4^2(z)+(z^3+z^2)B_5^2(z)\right|_{P^2(z)}^{+} =$$

$$= z^9+z^8+z^6+z^5+z^4+z^3; \quad deg\, M_2^*(z) > deg\, P_{раб}(z)$$

Следовательно, остаток $\alpha_2(z)=1$ не является ложным.

Удалим остаток $\alpha_3^{ложс}(z)=1$. Тогда M*(z)=(1, 1, z3+z2+z+1, z3+z2). В полученной системе модулей p1(z)=z+1; p2(z)=z2+z+1, p4(z)=z4+z3+1, p5(z)=z4+z+1 диапазон P3(z)=z11+z10+z6+z5+z+1.

Ортогональные базисы равны
B13(z)=z10+z5+1,
B23(z)=z9+z7+z6+z3+z2+1,
B43(z)=z8+z4+z2+z;
B53(z)=z10+z9+z8+z7+z6+z5+z4+ z3+z+1.

Тогда

$$M_3^* = \left|1B_1^3(z)+1B_2^3(z)+(z^3+z^2+z+1)B_4^3(z)+(z^3+z^2)B_5^3(z)\right|_{P^3(z)}^{+} =$$

$$= z^6 \quad deg\, M_3^*(z) < deg\, P_{раб}(z).$$

Следовательно, остаток $\alpha_3(z)=1$ является ложным.

Удалим остаток $\alpha_4(z)$. Тогда M*(z)=(1, 1, 1, z3+z2). В полученной системе с основаниями p1(z)=z+1, p2(z)=z2+z+1, p3(z)=z4+z3+z2+z+1, p5(z)=z4+z+1 диапазон P4(z)=z11+z10+z9+z8+z6+z4+z3+1.

Ортогональные базисы равны
B14(z)=z10+z8+z5+z4+z2+z+1,

B24(z)=z10+z9+z7+z4+z2+1,
B34(z)=z8+z4+z2+z;
B54(z)=z9+z7+z5+z4+z2+1.

Тогда

$$M_4^* = \left| 1B_1^4(z) + 1B_2^4(z) + 1B_3^4(z) + (z^3 + z^2)B_5^4(z) \right|_{P^4(z)}^{+} =$$

$$= z^{10} + z^9 + z^5 + z + 1; \quad deg\, M_4^*(z) > deg\, P_{раб}(z).$$

Следовательно, остаток $\alpha_4(z)$ не является ложным.

Таким образом, приведенный пример показал возможность разработанной системы разделения секретов обнаруживать и удалять ложный образ.

ЛИТЕРАТУРА

Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] / М.: − Издательство ТРИУМФ, − 2003. – 816 с.