Доказательство с нулевым разглашением для взаимной аутентификации пользователей группового чата

Нгуен Кхань Кхуен
421 группа

Научный руководитель:
к.ф.-м.н., с.н.с. Д.Ю.Гамаюнов

Постановка задачи

1. Провести исследование и сравнительный анализ протоколов доказательства с нулевым разглашением и оценить их применимость для взаимной аутентификации пользователей группового криптографического чата.
2. Предложить алгоритм групповой взаимной аутентификации на основе доказательства с нулевым разглашением и протокол на его основе.
3. Реализовать предложенный алгоритм для модельной системы на основе mpOTR.
4. Провести экспериментальное исследование предложенного алгоритма.

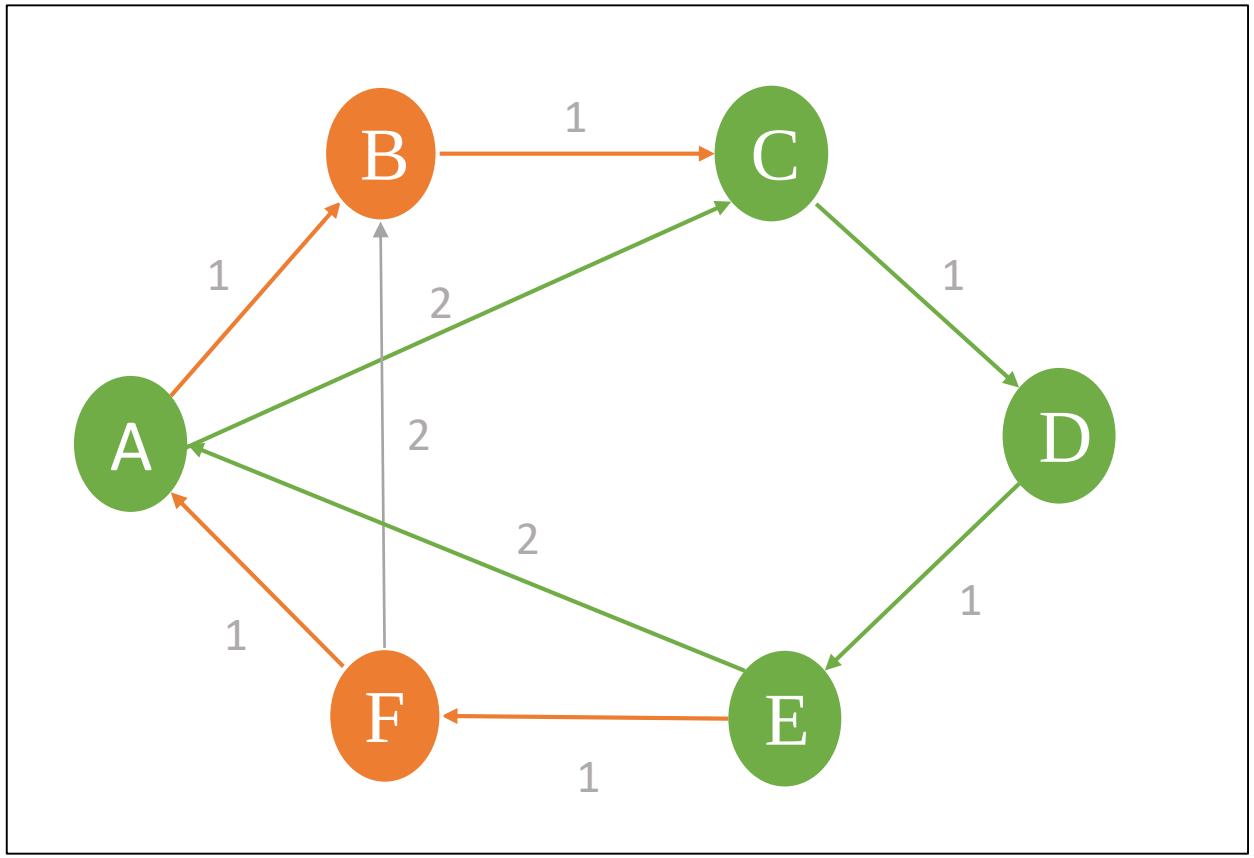
Протокол Миллионеров-Социалистов (SMP)

Генерация	Обмен	Вычисление
Алиса		Боб
a_2		b_2
$g_1^{a_2}$		$g_1^{b_2}$
$g_2 = g_1^{a_2 b_2}$		
a_3		b_3
$g_1^{a_3}$		$g_1^{b_3}$
$g_3 = g_1^{a_3 b_3}$		
a		b
$P_a = g_3^a, Q_a = g_1^a g_2^x$		$P_b = g_3^b, Q_a = g_1^b g_2^y$
$R_a = \left(\frac{Q_a}{Q_b}\right)^{a_3}$		$R_b = \left(\frac{Q_a}{Q_b}\right)^{b_3}$
$R_{ab} = \left(\frac{Q_a}{Q_b}\right)^{a_3 b_3} = \left(\frac{P_a}{P_b}\right)(g_2^{a_3 b_3})^{x-y}$		

Алгоритм:

1. Создание генераторов
2. Упаковка секретов x и y
3. Проверка x=y

Круговая аутентификация



1. Образование ориентированного кольца
2. Инициализация SMP со следующим участником
3. Рассылка результатов
4. Обновление таблицы доверенных участников
5. Шаг 2 при неуспешном SMP

Экспериментальное исследование

	Полная аутентификация	Круговая аутентификация
Кол-во раундов	n-1	$2 + 2p$
Выч. сложность	$O(n^2)$	$O(n)$
Количество сообщений	$2(n^2 - n)$	$n^2 + (3 + 4p)n - p$

Количество участников	Полная аутентификация - Время (мс)	Круговая аутентификация - Время (мс)
3	2646	2379
4	4120	3217
5	6736	3982
7	14088	5598
9	26886	8734

Результаты работы

1. Проведено исследование и сравнительный анализ протоколов Доказательства с нулевым разглашением.

2. Предложен протокол для групповой взаимной аутентификации на основе протокола Миллионеров-Социалистов.

3. Предложенный протокол реализован для модельной системы на основе mpOTR.

4. Проведено экспериментальное исследование предложенного протокола Круговой аутентификации.