# Схема подписи Фиата-Шамира.

Сначала генерируем n равное произведению двух простых чисел *p* и *q*. Далее выбирается *k* чисел *v*1,*v*2, .., *vk* являющимися квадратичными остатками по модулю *n*. Иными словами *vi* выбирается так чтобы *x*2 ≡ *vi*(mod *n*) имело решение и существовало *vi*-1 mod *n*. Значения *v*1,…*vk* будут являться открытым ключом. Затем вычисляются *s*2*i*≡ *vi*-1  mod *n*. Числа *s*1, …, *sk* будут являться закрытым ключом.

Генерация подписи:

1. А: {x}, где , r – случайное число Алисы

2. A:{}, где – первые k бит хэш-значения

3. А:{y}, где ,

4. А ->B:{m,, y}

Проверка подписи:

5. B: {z}, где

6. B: {}, где – первые k бит хэш-значения

7. B: проверяет, что {}=