ПРОТОКОЛЫ ИДЕНТИФИКАЦИИ

+ личностная криптография(ID-Based)

Протоколы идентификации на базе ZKP

- Пользователь должен убедить всех что он знает секрет, не раскрывая его и не передавая по сети.

- Область применения:
  - Вход с систему
  - Голосование (ЦУР)
  - Электронные платежи

Feige-Fiat-Shamir Identification Protocol (1998)

- 1. ***Setup***.
  - (a) Выбор системных параметров:
    - Доверенный центр T выбирает и публикует модуль RSA $n = pq$, но сохраняет p и q в секрете.
  - (b) Выбор индивидуальных секретов:
    - Каждый Prover A выбирает k секретов $s_1, s_2, ..s_k$, $1 \le s_i \le n - 1$, и k случайных бит $b_1, \ldots b_k$ и вычисляет

      $v_i = (-1)^{b_i} (s_i^2)^{-1} \bmod n$, $1 \le i \le k$.
    - Prover передает ($v_1 \ldots v_k$, n) доверенному центру T как свой публичный ключ.

Feige-Fiat-Shamir Identification Protocol

- 2. Работа протокола
  - a) A выбирает число r, бит b, вычисляет $x=(-1)^b r^2 \bmod n$, отсылает x (*свидетеля*) B
  - b)B отсылает A *запрос* случайный k-битовый вектор($e_1,e_2,...e_k$)
  - c)A вычисляет $y=r\prod_{j=1}^{k} s_j^{e_j} \bmod n$ и отправляет y B (*ответ*)
  - d)B вычисляет $z=y^2\prod_{j=}^{k} v_j^{e_j} \bmod n$. И проверяет $z= \pm x$ и $z \neq 0$

Пример работы протокола Feige-Fiat-Shamir Identification

- 1. Центр T выбрал простые числа p = 683, q = 811, и опубликовал n = pq = 553913. Числа k = 3 и t = 1 выбраны параметрами секретности.
- 2. Сторона A выполняет следующие шаги:
  - (a) Выбирает 3 случайных числа s_1=157, s_2= 43215, s_3 = 4646, и 3 бита b_1 = 1, b_2 = 0, b_3 = 1.
  - (b) Вычисляет v_1 = 441845, v_2 = 338402, и v_3 = 124423.
  - (c) Публичный ключ A равен (441845, 338402, 124423, 553913), а его секретный ключ (157, 43215, 4646).
- 3. Шаги протокола:
  - (a) A выбирает r = 1279, b = 1, вычисляет x = 25898, отправляет его B.
  - (b) B передает A 3-битный вектор (0, 0, 1).
  - (c) A вычисляет ответ $y = r\, s_3 \bmod n$ = 403104 и отправляет его B.
  - (d) B вычисляет $z = y^2\, v_3 \bmod n$ = 25898 и признает A, так как z = +x and $z \neq 0$.

Guillou-Quisquater (GQ) Identification Protocol (1988)

- Параметры системы
  - Секретные: p, q, $s=v^{-1} \bmod \phi(n)$
  - Публичные: n=pq, v >2
- Параметры пользователя
  - У пользователя A с идентификатором $J_A=f(I_A)$, секрет равен $J_A^{-s} \bmod n$
- Один цикл протокола(Повторяется *t* раз)
  - A отсылает B(Commit): I_A, $x=r^v \bmod n$ для случайного значения r
  - B отсылает A(Challenge): случайное *e*, такое что 1=<e=<v
  - A отсылает B(Response): $y=r\, s_A^e \bmod n$
- Проверка
  - B вычисляет $z=J_A^e y^v \bmod n$
  - Принимает доказательство A, если $z = x$ and $z \neq 0$

Schnorr Identification Protocol (1990)

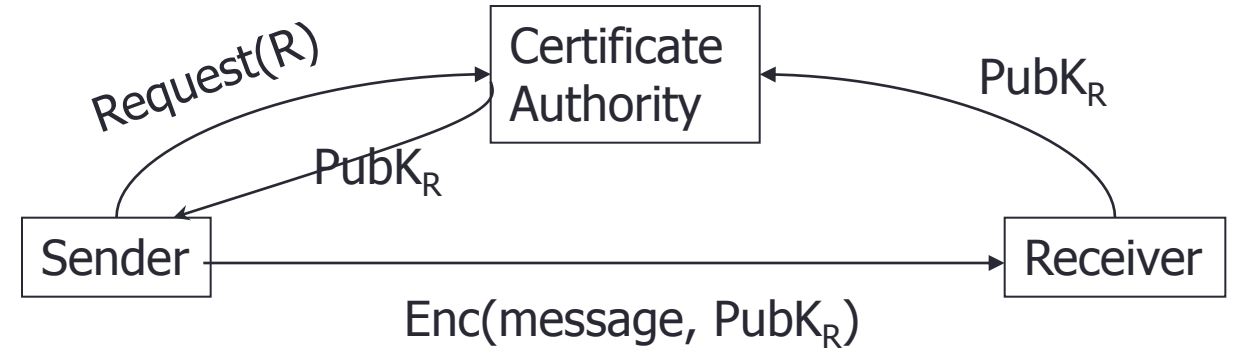
- Параметры системы
  - Простые числа p и q, такие что q|p-1
  - $h=g^{(p-1)/q} \bmod p$ имеет порядок q (g порождающий элемент GF(p))
  - Публичный проверочный ключ $S_T(m)$, параметр безопасности *t*
- Параметры пользователей
  - A выбирает секретный ключ *a* и вычисляет публичный ключ $v=h^{-a}$
  - A передает v на хранение T и получает сертификат $cert_A=(I_A,v,S_T(I_A,v))$

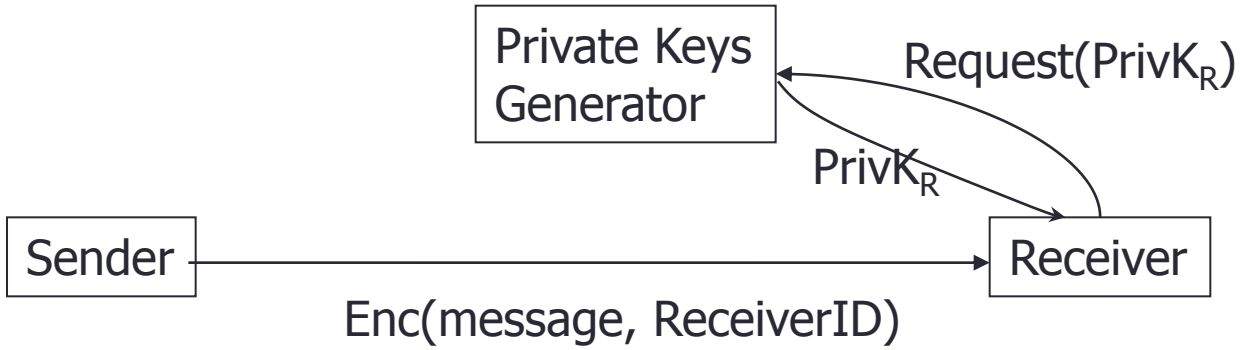
Schnorr Identification Protocol

- Раунд протокола(повторяется *t* раз)
  - A посылает B(Commit): $cert_A$, $x=h^r \bmod p$ для случайного *r*
  - B проверяет публичный ключ A и отправляет (Challenge): случайное *e* : $1=<e=<2^t<q$
  - A отсылает B(Response): $y=ae+r \bmod q$
- Проверка
  - B вычисляет $z=h^y v^e \bmod p$
  - И принимает доказательство A, если z=x

Личностная криптография

Традиционная схема PKI и личностная криптография (ID-Based)

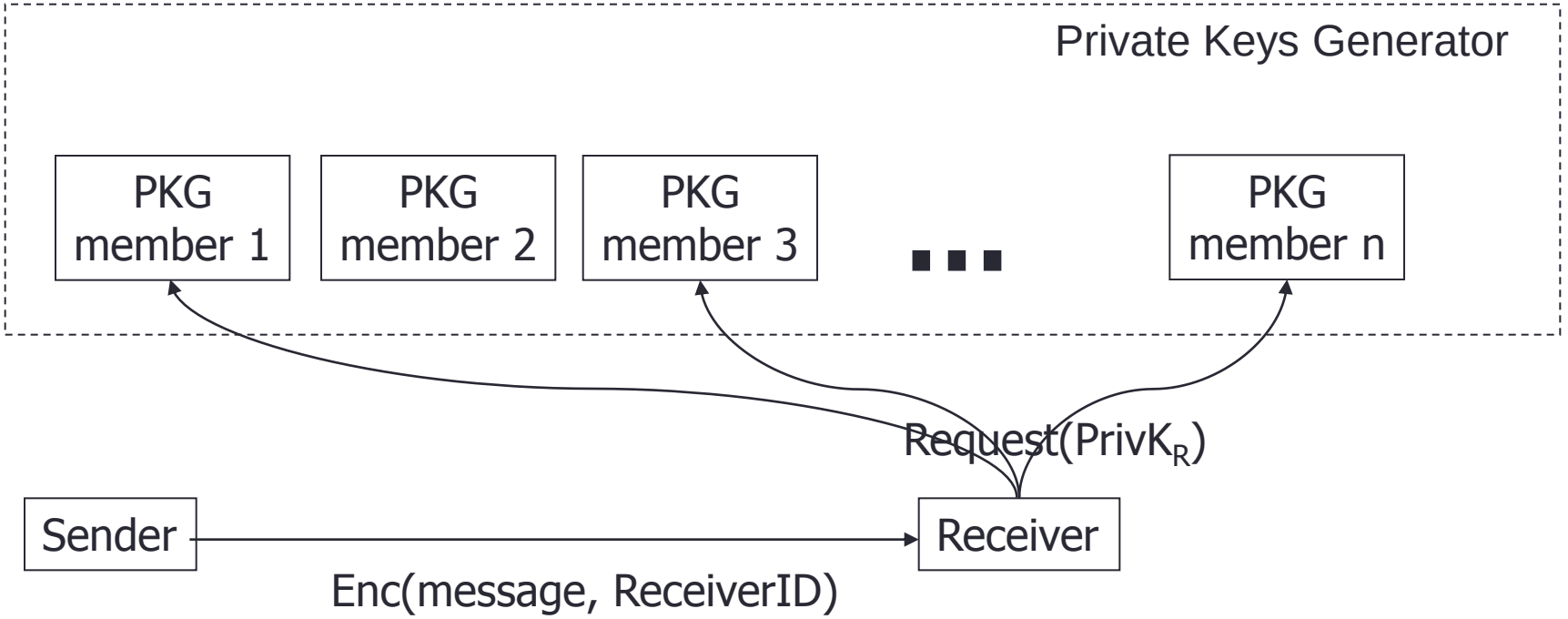




- Отправителю больше не нужно запрашивать PK получателя
- Снижается нагрузка на доверенный сервер

Единственная точка уязвимости PKG

Пороговая личностная криптография



- Распределенная процедура генерации секретных ключей повышают надежность и безопасность системы

Formal Definitions

- Id-Based Encryption
  - Setup(σ)
  - Extract(MSK, ID)
  - Encrypt(m, ID, PK)
  - Decrypt(c, sk_id, PK)
- (l,n)-Threshold Id-Based Encryption
  - Setup(l,n, σ)
  - ShareKeyGen(PK, i, SK_i, ID)
  - Combine(PK, ID, (H1…Hl))
  - Encrypt(m, ID, PK)
  - Decrypt(c, sk_id, PK)

Существующие подходы

- Эллиптические кривые
  - Threshold modifications exist
  - Small length of ciphertext
  - High calculation complexity
- Системы на решетках
  - Small calculation complexity
  - Very long ciphertext
  - There is non-zero probability of decryption error
- Системы на квадратичных вычетах
  - The smallest calculation complexity
  - There is no threshold scheme

Система IBE Cocks

- Основная идея – использование QR проблемы, если

$M = pq$ и $\left(\frac{x}{M}\right) = 1$, x is QR or NQR?

- Публичный ключ пользователя – Hash(ID) = a
- Секретный ключ – r: $r^2 = a$ or $-a$
- Вычисление секретного ключа: $r = a^{1/2} \bmod M$