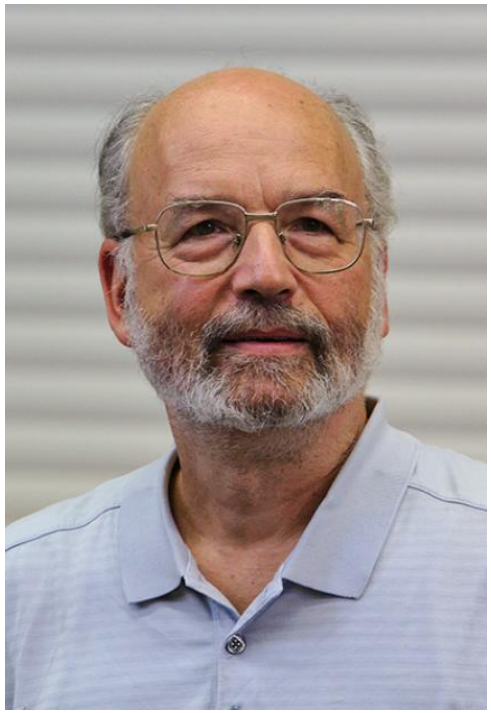
Аутентификация на основе доказательства с нулевым разглашением

Уриэль Фейге (1959 г., Израиль)

Амос Фиат (1956 г., Израиль)



Ади Шамир (1952 г., Израиль)

Использовать доказательства с нулевым знанием для проведения аутентификации было впервые предложено Уриелем Фейге (Uriel Feige), Амосом Фиатом (Amos Fiat) и Ади Шамиром (Adi Shamir) в 1986 году. В данном случае пользователь доказывает знание своего закрытого ключа, который выступает в роли секрета, не раскрывая его. Тем самым он доказывает свою аутентичность.

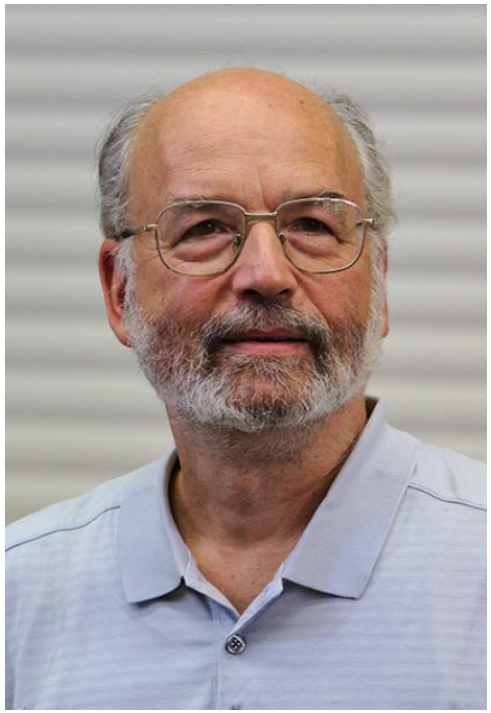
Фейге, Фиат и Шамир модифицировали ранее предложенный алгоритм Фиата и Шамира цифровой подписи и проверки подлинности, превратив его в доказательство подлинности с нулевым разглашением.

Аутентификация на основе доказательства с нулевым разглашением

Схемы аутентификации

Уриэль Фейге (1959 г., Израиль)

Амос Фиат (1956 г., Израиль)



Ади Шамир (1952 г., Израиль)

Схемы аутентификации содержат три этапа:

1) генерация общих параметров системы;
2) генерация индивидуальных параметров системы;
3) собственное тело протокола.

Генерация общих и индивидуальных параметров проводится независимой стороной, поэтому все схемы аутентификации являются протоколами с посредником.

Аутентификация на основе доказательства с нулевым разглашением

Схема аутентификации Фейге-Фиата-Шамира

Генерация общих параметров. Доверенный центр T (Трент) публикует большое число $n = p \cdot q$, где p, q — большие простые числа, которые держатся в секрете. (Использование чисел Блюма облегчит вычисления, но не является обязательным для безопасности, надёжность протокола основана на сложности извлечения дискретного квадратного корня). Также выбираются целые числа k и t — параметры безопасности.

Генерация индивидуальных параметров. A (Алиса) выбирает k случайных целых чисел $s_1, s_2, \ldots, s_k$, $1 \le s_i \le n - 1$ и k случайных бит $b_1, b_2, \ldots, b_k$. Затем вычисляет $v_i = (-1)^{b_i} (s_i^2)^{-1} \bmod n$, где $1 \le i \le k$. Алиса идентифицирует себя окружающим с помощью значений $v = (v_1, v_2, \ldots, v_k, n)$, которые выступают в качестве её открытого ключа, в то время как секретный ключ $s = (s_1, s_2, \ldots, s_k)$ известен только самой Алисе.

Аутентификация на основе доказательства с нулевым разглашением

Схема аутентификации Фейге-Фиата-Шамира

Протокол. Алиса доказывает своё знание секрета s Бобу в течение t раундов, не раскрывая при этом ни одного бита самого секрета. Действие протокола в рамках одного раунда (одной аккредитации):

1. $A \to B$:{x}, где $x = (-1)^b (r^2) \bmod n$, r – новое случайное число Алисы, $1 \le r \le n-1$, b – случайный бит Алисы;
2. $B \to A$: {(e_1, e_2, …, e_k)}, где e_i – случайные биты Боба;
3. $A \to B$:{y}, где $y = r \cdot (s_1^{e_1} \cdot s_2^{e_2} \cdot \ldots \cdot s_k^{e_k}) \bmod n$, (перемножает значения s_i, соответствующие $e_i = 1$);
4. B: Боб вычисляет $z = y^2 \cdot (v_1^{e_1} \cdot v_2^{e_2} \cdot \ldots \cdot v_k^{e_k}) \bmod n$ (перемножает значения v_i, соответствующие $e_i = 1$) и проверяет $z = \pm x$ и $z \neq 0$.

ЗАМЕЧАНИЕ 1. Вероятность успешной атаки на протокол составляет 2^{-kt}.

Аутентификация на основе доказательства с нулевым разглашением

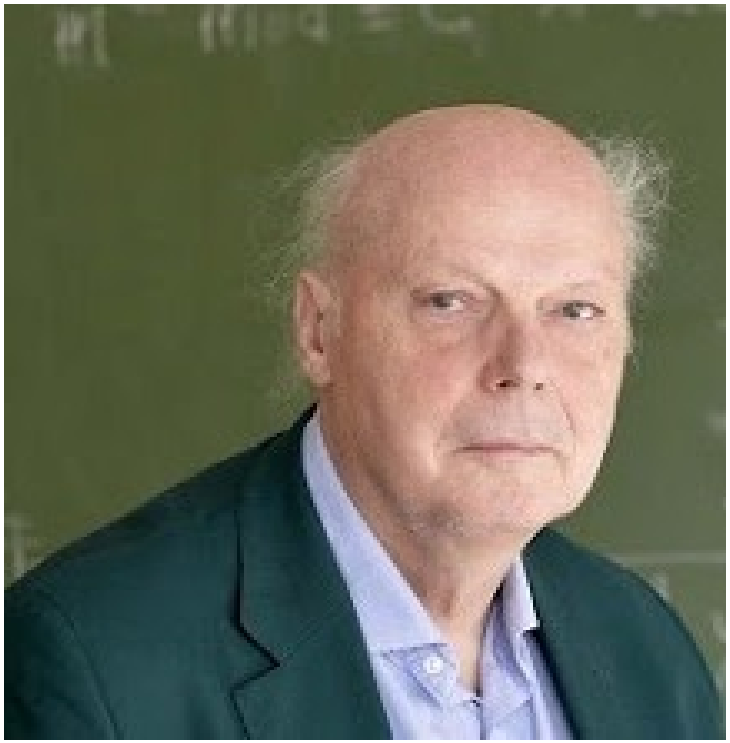
Схема аутентификации Фейге-Фиата-Шамира

ЗАМЕЧАНИЕ 2. Схему можно изменить так, чтобы она основывалась на идентичности каждого участника. Для этого пользователю A доверенный центр T назначает уникальную идентифицирующую строку I_A с информацией об участнике A (например, имя, адрес, номер паспорта и т. д.). Затем T вычисляет значения $v_i = f(I_A, a_i)$, $1 \le i \le k$, где f должна быть неотличима от случайной функции за полиномиальное время, и a_i небольшие числа выбираются так, чтобы $f(I_A, a_i)$ являлось квадратичным вычетом по модулю n. Потом, зная факторизацию n, T вычисляет $s_i = \sqrt{v_i^{-1}} \bmod n$ и выдает их значения A. Значения $v = (v_1, v_2, \ldots, v_k, n)$ и $s = (s_1, s_2, \ldots, s_k)$ становятся, соответственно, открытым и секретным ключами участника A.

Аутентификация на основе доказательства с нулевым разглашением

Схема аутентификации Гиллу-Кискате

Луи Гилу
(Louis Claude Guillou, 1947 г. Франция)



Жан-Жак Кискатер
(Jean-Jacques Quisquater, 1945 г. Бельгия)

Аутентификация на основе доказательства с нулевым разглашением

Схема аутентификации Гиллу-Кискате

Генерация общих параметров. Доверенный центр T (Трент) публикует большое число $n = p \cdot q$, где p, q — большие различные простые числа, которые держатся в секрете.

Генерация индивидуальных параметров.

1) T выбирает целое число e ($1 < e < \varphi(n)$), взаимно простое с $\varphi(n)$, где $\varphi(n) = (p - 1)(q - 1)$ — функция Эйлера;
2) T вычисляет $s = e^{-1} (\mathrm{mod}\ \varphi(n))$ и $x = J^{-s} (\mathrm{mod}\ n)$, где J — битовая строка личной информации о пользователе A, с условием $(J, n) = 1$;
3) T вычисляет $y = x^{e} \ (\mathrm{mod}\ n)$;
4) Тройка $\{n, e, y\}$ публикуется в качестве открытого ключа A, а x является закрытым ключом пользователя A.

Аутентификация на основе доказательства с нулевым разглашением

Схема аутентификации Гиллу-Кискате

Протокол. Алиса доказывает своё знание секрета x Бобу в течение одного раунда (одной аккредитации):

1. $A \to B$: $\{a\}$, где $a = r^e \bmod n$, r — случайное число Алисы, $1 \le r \le n - 1$;
2. $B \to A$: $\{c\}$, где c — случайное число Боба, $0 \le c \le e - 1$;
3. $A \to B$: $\{z\}$, где $z = r \cdot x^c \bmod n$,;
4. B: Боб проверяет, что $z^e = a \cdot y^c \bmod n$.

ЗАМЕЧАНИЕ. Безопасность протокола основана на сложности извлечения дискретного корня степени e по модулю достаточно большого составного числа n. В сравнении с протоколом Фейге-Фиата-Шамира протокол Гиллу-Кискате имеет меньшее число сообщений, которыми необходимо обменяться сторонам для проведения аутентификации. Протокол требует только один раунд обмена сообщениями, имеет более низкие требования к памяти, используемой для хранения секретов пользователей, однако требует большего объёма вычислений.

Аутентификация на основе доказательства с нулевым разглашением

Схема аутентификации Шнорра

Клаус-Петер Шнорр (нем. Claus-Peter Schnorr**,** род. 4 августа 1943 г.) — немецкий математик и криптограф.

Он получил докторскую степень в Университете Саарбрюккена в 1966 году. Вклад Шнорра в криптографию включает его исследование групп Шнорра, которые используются в алгоритме цифровой подписи, носящем его имя. Помимо этого, Шнорр известен своим вкладом в алгоритмическую теорию информации и созданием подхода к определению алгоритмически случайной последовательности, который является альтернативой концепции случайности Мартина-Лёфа.

Шнорр был профессором математики и информатики в университете Иоганна Вольфганга Гете во Франкфурте. Он ушел на пенсию в 2011 году, проработав там 40 лет. Он также является заслуженным сотрудником лабораторий RSA и одним из лауреатов премии Готфрида Вильгельма Лейбница вместе с Йоханнесом Бухманном в 1993 году. Вместе с Жан-Жаком Кискате он получил премию RSA за выдающиеся достижения в области математики в 2013 году.

Аутентификация на основе доказательства с нулевым разглашением

Схема аутентификации Шнорра

Генерация общих параметров. Доверенный центр *T* (Трент) в схеме проверки подлинности Клауса Шнорра (Claus Schnorr) для генерации пары ключей вначале выбирает два простых числа, *p* и *q* так, чтобы *q* было делителем $p - 1$. Далее выбирается значение *a*, не равное 1, такое, что $a^q \equiv 1 \pmod{p}$. Все эти числа $\{p, q, a\}$ могут быть свободно опубликованы и использованы группой пользователей.

Генерация индивидуальных параметров.

Для генерации отдельной пары ключей выбирается случайное число *s*, меньшее *q*. Затем вычисляется $v = a^{-s} \bmod p$. Закрытым ключом Алисы является *s*, открытым ключом Алисы является *v*.

Аутентификация на основе доказательства с нулевым разглашением

Схема аутентификации Шнорра

Протокол. Алиса доказывает своё знание секрета s Бобу в течение одного раунда (одной аккредитации):

1. $A \to B$: $\{x\}$, где $x = a^r \bmod p$, r — случайное число Алисы, $1 \le r \le q - 1$;
2. $B \to A$: $\{e\}$, где e — случайное число Боба, $0 \le e \le 2^t - 1$. (t – параметр надёжности);
3. $A \to B$: $\{y\}$, где $y = (r + se) \bmod q$;
4. B: Боб проверяет, что $x = a^y v^e \bmod p$.

ЗАМЕЧАНИЕ. Безопасность схемы аутентификации Клауса Шнорра базируется на трудоемкости вычисления дискретных логарифмов. Безопасность алгоритма также зависит от параметра t. Сложность вскрытия алгоритма примерно равна 2^t. Шнорр советует использовать значение p, длиной примерно 1024 битов, q — примерно 160 битов и t — 72.

Аутентификация на основе доказательства с нулевым разглашением

Схема аутентификации Шнорра

Протокол. Алиса доказывает своё знание секрета s Бобу в течение одного раунда (одной аккредитации):

1. $A \to B$: $\{x\}$, где $x = a^r \bmod p$, r — случайное число Алисы, $1 \le r \le q - 1$;
2. $B \to A$: $\{e\}$, где e — случайное число Боба, $0 \le e \le 2^t - 1$. (t – параметр надёжности);
3. $A \to B$: $\{y\}$, где $y = (r + se) \bmod q$;
4. B: Боб проверяет, что $x = a^y v^e \bmod p$.

ЗАМЕЧАНИЕ. Безопасность схемы аутентификации Клауса Шнорра базируется на трудоемкости вычисления дискретных логарифмов. Безопасность алгоритма также зависит от параметра t. Сложность вскрытия алгоритма примерно равна 2^t. Шнорр советует использовать значение p, длиной примерно 1024 битов, q — примерно 160 битов и t — 72.

Аутентификация на основе доказательства с нулевым разглашением

Преобразование схем аутентификации в схемы подписи

Стандартный метод преобразования схемы аутентификации в схему подписи таков:

1. Боб (Проверяющий) заменяется однонаправленной хэш-функцией.
2. Перед подписанием сообщение не хэшируется, вместо этого хэширование встраивается в алгоритм подписи.

В принципе, такое преобразование можно проделать с любой схемой аутентификации.

Аутентификация на основе доказательства с нулевым разглашением

Схема подписи Фейге-Фиата-Шамира

Всякая схема подписи состоит из двух этапов, этапа генерации подписи и этапа проверки подписи. Генерация общих и индивидуальных параметров та же, что и в соответствующем протоколе аутентификации. Их содержание: $v = (v_1, v_2, \ldots, v_k, n)$ — открытый ключ A, $s = (s_1, s_2, \ldots, s_k)$ — закрытый ключ A.

Протокол. Алиса подписывает своё сообщение m, используя свою пару открытого и закрытого ключа. Боб проверяет подпись Алисы, используя её открытый ключ.

Генерация подписи.

1. $A : \{x\}$, где $x = r^2 \bmod n$, r – случайное число Алисы, $1 \le r \le n - 1$;
2. $A : \{(e_1, e_2, \ldots, e_k)\}$, где $e_i = h(x \| m)$ — первые k бит хэш-значения;
3. $A : \{y\}$, где $y = r \cdot (s_1^{e_1} \cdot s_2^{e_2} \cdot \ldots \cdot s_k^{e_k}) \bmod n$, (перемножает значения s_i, соответствующие $e_i = 1$);
4. $A \to B$: $\{m, (e_1, e_2, \ldots, e_k), y\}$.

Проверка подписи.

5. $B : \{z\}$, где $z = y^2 \cdot (v_1^{e_1} \cdot v_2^{e_2} \cdot \ldots \cdot v_k^{e_k}) \bmod n$ (перемножает значения v_i, соответствующие $e_i = 1$);
6. $B : \{(e_1^*, e_2^*, \ldots, e_k^*)\}$, где $e_i^* = h(z \| m)$ — первые k бит хэш-значения;
7. B : проверяет, что $(e_1^*, e_2^*, \ldots, e_k^*) = (e_1, e_2, \ldots, e_k)$.

Аутентификация на основе доказательства с нулевым разглашением

Схема подписи Гиллу-Кискате

Генерация общих и индивидуальных параметров та же, что и в соответствующем протоколе аутентификации. Их содержание: $\{n, e, J\}$ — открытый ключ A, J — битовая строка личной информации о пользователе A, а x — закрытый ключ A.

Протокол. Алиса подписывает своё сообщение m, используя свою пару открытого и закрытого ключа. Боб проверяет подпись Алисы, используя её открытый ключ.

Генерация подписи.

1. $A : \{a\}$, где $a = r^e \bmod n$, r – случайное число Алисы, $1 \le r \le n - 1$;
2. $A : \{d\}$, где $d = h(m \| a) \bmod e$;
3. $A : \{z\}$, где $z = r \cdot x^d \bmod n$;
4. $A \to B$: $\{m, d, z, J\}$.

Проверка подписи.

5. $B : \{a^*\}$, где $a^* = z^e \cdot J^d \bmod n$;
6. $B : \{d^*\}$, где $d^* = h(m \| a^*) \bmod e$;
7. B : проверяет, что $d^* = d$.

Аутентификация на основе доказательства с нулевым разглашением

Схема подписи Шнорра (Схема цифровой подписи)

Генерация общих и индивидуальных параметров та же, что и в соответствующем протоколе аутентификации. Их содержание: $\{p, q, a\}$ — общие параметры; v. — открытый ключ A, s — закрытый ключ A.

Протокол. Алиса подписывает своё сообщение m, используя свою пару открытого и закрытого ключа. Боб проверяет подпись Алисы, используя её открытый ключ.

Генерация подписи.

1. $A : \{x\}$, где $x = a^r \bmod p$, r — случайное число Алисы, $1 \le r \le q - 1$;
2. $A : \{e\}$, где $e = h(m \| x)$ — первая подпись;
3. $A : \{y\}$, где $y = (r + se) \bmod q$ — вторая подпись;
4. $A \to B$: $\{m, e, y\}$.

Проверка подписи.

5. $B : \{x^*\}$, где $x^* = a^y \cdot v^e \bmod p$;
6. B : проверяет, что $e = h(m \| x^*)$.