# СХЕМА СЛЕПОЙ ПОДПИСИ НА ОСНОВЕ ГОСТ Р 34.10-94

***Жумаев Тавлонбек***
*Национальный университет Узбекистана имени Мирзо Улугбека Прикладная математика и интеллектуальные технологии Студент 1 курса магистратуры по специальности «криптография и криптоанализ» (по направлениям)*

**Аннотация-** Подробно поясняется схема слепой подписи по ГОСТ 34.10-94. На данной схеме показано, как подписывать схему на примерах

**Abstract-** This GOST 34.10-94 blind signature scheme is explained in detail. This scheme shows how to sign the scheme in examples

**Ключевые слова:** слепой подписи,протокол,алгоритм,ключ

**Keywords:** Blind signature,protocol,algorithms,key

Стандарт ЭЦП ГОСТ Р 34.10-94 рекомендует использование простого числа $p$, такого что $510 \le |p| \le 512$ бит либо $1022 \le |p| \le 1024$ бит, где $|p|$ — разрядность числа $p$ в двоичном представлении, причем число $p$ - 1 содержит большой простой делитель, $2^{255} \le 7 \le 2^{256}$ либо $2^{511} \le 7 \le 2^{512}$ соответственно. Специфицируемые алгоритмы генерации и проверки ЭЦП используют число $\alpha < p$, такое что $a \neq 1$ и $a^q \bmod p = 1$. Вычисление ЭЦП осуществляется следующим образом:

1. Генерируется случайное число $k$, $1 < k < q$.
2. Вычисляется значение $K = (\alpha^q \bmod p)$, являющееся первой частью подписи.
3. По стандарту ГОСТ Р 34.11-94 вычисляется хэш-функция $H$ от подписываемого сообщения.
4. Вычисляется вторая часть подписи: $S = kH + zR \bmod q$, где $z$ — секретный ключ.

Если S=0, процедура генерации подписи повторяется. Процедура проверки подлинности ЭЦП:

1. Поверяются выполнение условий $r < q$ и $s < q$. Если они не выполняются, то подпись признается недействительной.
2. Вычисляется значение

$$R' = (\alpha^{S/H} y^{R/H} \bmod p) \bmod q.$$

3. Сравниваются значения $R$ и R'. Если R = R', то подпись признается действительной.

При построении протокола слепой подписи на основе стандарта ГОСТ Р 34.10-94, приводимого далее, используются два "ослепляющих" множителя,

задаваемых в виде yμ и aε, которые использовались при построении схемы слепой подписи на основе алгоритма ЭЦП Шнорра *(см. разд. 3.7).* Кроме того, используется два дополнительных "ослепляющих" параметра τ и δ, применение которых связано со спецификой проверочного уравнения, регламентируемого стандартом. Протокол слепой подписи на основе указанного стандарта реализуется следующим образом:

1. Подписывающий генерирует случайное число k<*q*, вычисляет значение $p = \alpha^{k} \ mod \ p$ и направляет его пользователю A, который намерен представить некоторое электронное сообщение *M* для получения слепой подписи.

2.Пользователь A генерирует случайные значения μ,ε,δ,τ,ϵ{1,2,..., *q* - 1}, вычисляет значения $p' = p^{1/\delta} y^{\mu} a^{e} \bmod p$, $R' = p' \bmod q$, $H = H'\tau \ mod \ q$ и $R = \delta\tau(R' + \mu H') \bmod q$, где *H'*— значение хэш-функции от подписываемого документа, вычисленное по стандарту ГОСТ Р 34.11-94 (или по другому специфицированному алгоритму вычисления хэш-функции, значение которой имеет размер не менее 160 бит). Значение R', которое остается неизвестным подписывающему, представляет собой первый элемент формируемой подписи.

3.Пользователь A отправляет подписывающему значения R и H, и з которых нельзя вычислить ни *R'*, ни *H',* поскольку для любой пары *(R', H')* существует пара значений (τ,μ), которые связывают (*R'*, *H'*) с полученной парой значений *(R, H).*

4.Подписывающий вычисляет значение $S = kH + zR \ mod \ q$, где z — его секретный ключ, передает вычисленный элемент слепой подписи пользователю A.

5. Пользователь A вычисляет значение $S' = \delta^{-1} \tau^{-1} S + \varepsilon H'$, которое является вторым элементом подписи.

Полученная в соответствии с этим протоколом ЭЦП (*R'*, *S'*) является подлинной, т. ё. она вместе с хэш-значением *H'* от сообщения *M* проходит уравнение проверки подписи, регламентируемое стандартом ГОСТ Р 34.10-94. Действительно, корректность описанного протокола доказывается следующим путем.

*Доказательство корректности.* Элемент слепой подписи S вычисляется на шаге 4 по формуле $S = kH + zR \bmod q$, из которой с учетом того, что число a имеет порядок *q* по модулю *p,* следует справедливость сравнения $\alpha^{S} = a^{kH} a^{zR} \bmod p$, из которого имеем $p = a^{k} = a^{S/H} \ a^{-zR/H} \bmod p$. Учитывая, что $R' = (\delta^{-1}\tau^{-1}R - \mu H') \bmod q$, вычислим правую часть проверочного уравнения в случае проверяемой подписи (*R'*, *S'*) и значения хэш-функции *H':*

$$(a^{S`/H`} \ y^{-R`/H`} \bmod p) \bmod q = (a^{\delta\text{-}1 \ \tau\text{-}1 \ S+\varepsilon H`/H`} \ y^{\delta\text{-}1 \ \tau\text{-}1 \ R-\mu H`/H`} \bmod p) \bmod q =$$

$= (a^{(S/\delta H`\tau)+\varepsilon} y^{(-R/\delta H`\tau)+\mu} \bmod p) \bmod q = ((a^{S/H} y^{-R/H})1/\delta\ a^{\varepsilon} y^{\mu} \bmod p) \bmod q = (p^{1/\delta} a^{\varepsilon} y^{\mu} \bmod p) \bmod q = p' \bmod q = R'.$

Правая часть проверочного уравнения равна элементу *R'* проверяемой подписи, следовательно, подпись *(R', S')* к сообщению *M* является подлинной.

Рассмотренный протокол обеспечивает анонимность пользователя, предоставляющего документ для получения коллективной подписи вслепую, т. е. при предъявлении подписи *(R', S')* к сообщению *M* подписавший не может установить пользователя, который предоставлял ему этот документ на подпись, с вероятностью выше значения *d/N*, где N— количество документов подписанных (данным подписывающим) с помощью протокола слепой подписи; d — число документов, предоставлявшихся данным пользователем. Это требование выполняется, если любая подпись *(R', S')* может быть с равной вероятностью отнесена к каждой из N выполненных процедур протокола слепой подписи (предполагается, что все значения, получаемые подписывающим в процессе протокола, регистрируются им). Описанный протокол удовлетворяет этому требованию.

Действительно, любая четверка значений (p, *K, 8, H)* из множества таких четверок, которые известны подписывающему, может быть ассоциирована с произвольной подлинной подписью

(*R', S'*) к произвольному сообщению, представленному значением хэш-функции *H'*. Это связано с тем, что четверка (p, R,*S, H)* и тройка (R', *S', H' )* в соответствии с протоколом связаны случайными параметрами μ, ε, δ и τ. Для произвольно заданных четверки и тройки значения μ, ε, δ и τ вычисляются однозначно следующим путем. Вычисляется множитель $\tau = H/ H' \bmod q$, значение $p' = a^{S/H} y^{-R/H} \bmod p$ и логарифм $L = \log_a p'$ по mod *p* (так как значение p' есть цело

численная степень числа a, то указанное значение логарифма существует и является единственным в области $L < q$). Учитывая, что $\log_a p' = k/\delta + z\mu + \varepsilon$, получаем следующую систему из трех линейных уравнений с тремя неизвестными $\delta^{-1}$, μ и ε:

$$k\,\delta^{-1} + z\mu + \varepsilon = L \bmod q$$
$$\delta^{-1} R\,\tau^{-1} - \mu H' = R' \bmod q.$$
$$\delta^{-1} S\,\tau^{-1} + \varepsilon H' = S' \bmod q$$

Вероятность того, что главный определитель этой системы равен нулю, пренебрежимо мала, а именно равна $q^{-1} < 2^{-160}$, поэтому практически всегда данная система будет иметь решение. Это означает, что подписывающий может ассоциировать данную тройку (R', *S', H'*) с каждой из сохраненных им (в процессе выполнения протокола слепой подписи) четверок (p, R,*S,H)*. При равновероятном случайном выборе значений μ, ε и τ на шаге 2 протокола

тройка(R', *S', H'),* сформированная по протоколу слепой подписи, с равной вероятностью могла бы быть порождена из любой тройки (p, *R, S, H),* фигурировавшей в одной из N выполненных процедур слепого подписывания сообщений.

**Используемая литература**


1. Н. А. Молдовян . Протоколы Коллективной Подписина Основе Свертки Индивидуальных Параметров 230 с
2. Tuan Nguyen Kim1, Duy Ho Ngoc2 and Nikolay A. Moldovyan Collective Signature Protocols For Signing Groups Based On Problem Of Finding Roots Modulo Large Prime Number
3. Moldovyan.N.A Digital Signature Scheme Based on a New Hard Problem // Computer Science Journal of Moldova 2008
4. Lee E, Park J.H. Crytanalysis of the public key Encryption Based on Braid Groups // Advances in Cryptology – Eurocrypt 2003 / Lecture Notes in Computer Science .Springer Verlag