Санкт-Петербургский политехнический университет Петра Великого
Институт прикладной математики и механики
Кафедра «Информационная безопасность компьютерных систем»

Курсовая работа
Короткая подпись на основе задачи Диффи-Хеллмана
по дисциплине
«Криптографические методы защиты информации»

Выполнил
студент группы 43609/5 Соболь С.С.

Проверил
профессор, д.т.н. Александрова Е.Б.

Санкт-Петербург
2019

Введение

Короткая подпись необходима в системах с ограниченными ресурсами по времени, энергопотреблению, пропускной способностью или если пользователю приходится вводить её вручную, то, желательно, чтобы подпись была минимально короткой.

В RSA длина подписи 1024 бита, а в стандарте DSA или ECDSA (DSA с эллиптическими кривыми) – 320 бит. Это много. Поэтому были разработаны и другие схемы, где при длине подписи приблизительно 160 бит достигается примерно такой же уровень защиты, как и в DSS.

Схемы короткой подписи

Обычно схема электронной подписи состоит их трёх этапов:

1. Gen, который берёт на вход параметр безопасности и выдаёт долговременные параметры, личный ключ d и соответствующий ему открытый ключ Q.

2. Sign, который берёт на вход долговременные параметры, сообщение X, личный ключ d и выдаёт электронную цифровую подпись s.

3. Verify, который берёт на вход сообщение X, долговременные параметры, открытый ключ Q, подпись s и выдаёт результат «да» или «нет», где «да» означает, что подпись к сообщению X была выработана с использованием личного ключа d и сообщение X не было изменено с момента выработки подписи, и «нет» означает обратное

Схемы короткой подписи

В настоящее время ведётся большое количество работ по улучшению производительности криптографических алгоритмов путём сокращения количества вычислений экспонент.

Многие из этих схем используют билинейные отображения

Схемы короткой подписи

Пусть G_1 и G_2 – циклические аддитивные группы порядка q. G_3 - циклическая мультипликативная группа того же порядка. Отображение e: G_1 x $G_2 \rightarrow G_3$ называется спариванием, если оно удовлетворяет следующим условиям.

Для любых $p_1, p_2 \in G_1$, любых $g_1, g_2 \in G_2$ и любых a, b $\in Z^*_q$ выполняются следующие свойства:

- Билинейность: $e(p_1+p_2,g_1)=e(p_1,g_1)e(p_2,g_1)$; $e(p_1,g_1+g_2)= e(p_1,g_1)e(p_1,g_2)$

следовательно, $e(ap_1,bp_2)=e(p_1,p_2)^{ab}$

- Невырожденность: e(p1,g1) ≠ 1

- Вычислимость: существует эффективный алгоритм вычисления $e(p_1,g_1)$

Подпись BLS (Boneh, Lynn, Shacham)

BLS - короткая схема электронной подписи. Но она ограничена группами, для которых можно определить билинейное отображение, которое является основной операцией при проверке подписи

Схема подписи состоит из трёх этапов:

- Генерация параметров: Выбираются открытые параметры (P, Q, H), где $P \epsilon G_1$. Q – ключ проверки, $H\{0,1\}^* \rightarrow G_1$ – хэш-функция. Закрытым параметром является ключ подписи d.
- Формирование подписи: Вычисляется M=H(message). Вычисляется S=dM, где S – подпись сообщения.
- Проверка: Вычисляется хэш полученного сообщения:M=H(message). Проверяется следующее условие: e(P, S)=e(Q, M), где e – билинейное отображение. Подпись является действительной, если выполняется равенство.

Подпись BLS (Boneh, Lynn, Shacham)

Основной проблемой данной подписи является то, что она использует специальные хэш-функции. Поэтому стали предлагаться схемы с MD5 и SHA-1

Новая цифровая подпись на основе билинейных отображений

Разработан новый алгоритм подписи, который решает предыдущую проблему, позволяя уже использовать неспециальные хэш-функции, такие как SHA-1. Данная схема также используют билинейные отображения.

- Генерация параметров: открытые параметры (G_1,G_2,e,n,P,H), где P ϵG_1 , G_1 =<P>, e: G_1 x $G_1 \rightarrow G_2$, H: $Z^{\infty}_2 \rightarrow Z^{\lambda}_2$, где $160 \leq \lambda \leq \log(n)$ -хэш-функция, такая как SHA-1, x – случайно выбранный закрытый ключ. Вычисляются открытые ключи: $P_{pub1}=x^2P$ и $P_{pub2}=2xP$
- Формирование подписи: Вычисляется $S=(H(M)+x)^{-2}P$

Новая цифровая подпись на основе билинейных отображений

- Проверка: $e(H(M)^2P+P_{pub1}+H(M)*P_{pub2},S)=e(P,P)$

Покажем это:

$$e((H(M)+x)^2,(H(M)+x)^{-2}P)=e(P,P)^{((H(M)+x))2*(H(M)+x)-2}=e(P,P)$$

Новая цифровая подпись на основе билинейных отображений

Сравнение времени работы данной схемы с BLS и ZSS из работы Sedat Akleyk, Baris Bulent, Omer Sever «Short Signature Scheme from bilinear pairing», где ZSS (Zhang, Safavi-Naini и Susilo) – похожая схема короткой подписи, основанной билинейном отображении:

Таблица 1 - Сравнение времени работы

	BLS	ZSS	Предложенная
Всё время (генерация ключа, подпись и проверка)	0,17	0,09	0.101

Подпись Nyberg-Rueppel

Известно множество стандартных конструкций подписей, которые используют функции, которые иногда требуют значительных вычислительных затрат, что не всегда является приемлемо для устройств с ограниченными ресурсами. Подпись Nyberg-Rueppel является схемой с восстановлением исходного сообщения после проверки подписи без использования хэш-функций

Подпись Nyberg-Rueppel

- Генерация параметров: Выбираются открытые параметры (P, Q), где P, Q – такие большие простые целые числа, что $P=uQ+1$ где u – малое. Закрытый ключ $x \in [1,Q-1]$, открытый ключ $Y=g^x \bmod P$, где g - образующая подгруппы из Z^*_p.
- Формирование подписи: Генерируется случайное $k \in [1, Q-1]$. Вычисляется $R=mg^k \bmod P$, где m - сообщение.Вычисляется $S=-k-xR' (\bmod Q)$, где $S \in [1,Q-1]$,$R'=R(\bmod Q)$. Подписью является пара (S,R).
- Проверка: Проверяющий получает пару (R, S) и удостоверяется, что $R \in [1,P-1]$. Если условие выполняется, то он восстанавливает сообщение следующим образом: $RY^s g^s=(mg^k)(g^x)^{r'} g^s=mg^{k+r'x+s}=m(\bmod P)$

Подпись Nyberg-Rueppel

Очевидно, что данная версия схема подписи уязвима к тому, что можно подобрать пару (R, S), которая подписывает сообщение, полученное после восстановления. Это сообщение не может быть выбрано злоумышленником заранее, но что не делает подпись более надёжной. Решением для данной проблемы является функция избыточности, которая схожа с хэш-функцией в схемах подписи с дополнением. Но также необходимо, чтобы данная функция избыточности была легко обратимой. В модифицированной версии высчитывается некое $\grave{m}=f(m)$, где f – функция избыточности. Таким образом, безопасность данной версии заключается в том, что трудно подобрать такие R и S, чтобы выход восстанавливающего алгоритма лежал в образе f, что делает выбор избыточной функции деликатной задачей

Подпись Nyberg-Rueppel

- Генерация параметров: Выбираются открытые параметры (P, Q), где P, Q – такие большие простые целые числа, что $P=uQ+1$ где u – малое. Закрытый ключ $x \in [1,Q-1]$, открытый ключ $y=g^x \bmod P$, где g - образующая подгруппы из Z^*_p. f - открытая функция избыточности.
- Формирование подписи: Генерируется случайное $k \in [1, Q-1]$. Вычисляется $R=f(m)g^k \bmod P$, где m - сообщение.Вычисляется $S=-xR+k \pmod Q$, где $S \in [1,Q-1]$,r'=r(modQ). Подписью является пара (S,R).
- Проверка: Проверяющий получает пару (R, S) и удостоверяется, что

$$\frac{R}{G^S Y^{-R}} = \frac{R}{G^{S-Rx}} = \frac{R}{G^k \bmod P} = f(m).$$

Если полученное равенство верно, то подпись действительна, и исходное сообщения восстанавливается путём взятия обратной от полученного значения

Подпись Nyberg-Rueppel

Таким образом, применение схемы осуществляется без использования хеш-функций, позволяет восстанавливать исходные сообщения, имеет более короткая подпись на коротких сообщениях. Длина подписи достигает примерно 240 бит.

Сравнение схем

Таблица 2 - Сравнение схем

	BLS	New short sign	Nyberg-Rueppel
Длина подписи	160 бит	160 бит	240 бит
Хэш-Функция	Специальные	MD5,SHA1	-
Восстановление сообщения	-	-	+
Количество билинейных отображений	2	1	0

Заключение

В ходе выполнение курсовой работы были рассмотрены различные схемы короткой подписи на основе задачи Диффи-Хеллмана, и было приведено сравнение данных схем. Были реализованы функции для формирования и проверки подписи на основе схемы Nyberg-Rueppel. Таким образом, можно сделать вывод, что короткая подпись удобна в использовании для пользователей и для систем, с ограниченными ресурсами, так как она не требует большого количества вычислений.