Об одном классе механизмов, предназначенных для одновременного шифрования и формирования подписи

Антон Гуселев

– CTCrypt 2024 –

Содержание

Идея создания signcryption-механизмов

Новая signcryption концепция

В 1997 году предложена новая концепция защиты информации, целью которой являлось одновременное обеспечение невозможности подделки подписи и нарушение конфиденциальности

Основные достоинства *(по словам авторов концепции)*

Сокращение трудоемкости реализуемых преобразований и информационных взаимодействий *(относительно signature-then-encryption)*

Y. Zheng. Digital Signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature) + Cost(Encryption). *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, 1997.

Идея создания signcryption-механизмов

Новая signcryption концепция

В 1997 году предложена новая концепция защиты информации, целью которой являлось одновременное обеспечение невозможности подделки подписи и нарушение конфиденциальности

Основные достоинства *(по словам авторов концепции)*

Сокращение трудоемкости реализуемых преобразований и информационных взаимодействий *(относительно signature-then-encryption)*

Существуют механизмы, способные решать схожую задачу

- варианты протокола Диффи-Хеллмана
- механизмы инкапсуляции ключа
- ...

однако signcryption отдельное направление со своими особенностями

Первоначальный вариант signcryption-механизма

**было предложено 2 варианта: SECDSS1 и SECDSS2*

Базовые условия

- пусть A хочет передать B сообщение m
- заданы ключи (d_A, Q_A), (d_B, Q_B), где $Q_A = d_A P$, $Q_B = d_B P$
- заданы функции $\mathrm{H}(\cdot)$ хеширования и $\mathrm{HK}_k(\cdot)$ ключевого хеширования
- заданы алгоритмы зашифрования и расшифрования $E_k(\cdot)$ и $D_k(\cdot)$

Signcryption SECDSS1

Вход: d_A, Q_B и сообщение m
Выход: ш.т. c и подпись (r, s)

1: Выбрать $k \in_R \{1, 2, \ldots, q-1\}$
2: Вычислить $(k_1, k_2) = \mathrm{H}(kQ_B)$
3: Вычислить $c = E_{k_1}(m)$
4: Вычислить $r = \mathrm{HK}_{k_2}(m)$
5: Вычислить $s = k(r + d_A)^{-1} \bmod q$

UnSigncryption SECDSS1

Вход: d_B, Q_A, ш.т. c и подпись (r, s)
Выход: о.т. и результат проверки

1: Вычислить $u = sd_B$
2: Вычислить $(k_1, k_2) = \mathrm{H}(uQ_A + urP)$
3: Вычислить $m = D_{k_1}(c)$
4: **Если** $\mathrm{HK}_{k_2}(m) = r$ **то** принять m
5: **иначе** отвергнуть m

Первоначальный вариант signcryption-механизма

**было предложено 2 варианта: SECDSS1 и SECDSS2*

Синтезные особенности

- в основе лежит вариант схемы подписи Эль-Гамаля
- в механизме SECDSS2 вычисляется $s = k(1 + d_A r)^{-1} \bmod q$
- модифицированный вариант схемы подписи ECDSA, где подписывается такое сообщение, что $\mathrm{H}(\mathrm{Msg}) = 1$

Signcryption SECDSS1

Вход: d_A, Q_B и сообщение m
Выход: ш.т. c и подпись (r, s)

1: Выбрать $k \in_R \{1, 2, \ldots, q-1\}$
2: Вычислить $(k_1, k_2) = \mathrm{H}(kQ_B)$
3: Вычислить $c = E_{k_1}(m)$
4: Вычислить $r = \mathrm{HK}_{k_2}(m)$
5: Вычислить $\boxed{s = k(r + d_A)^{-1} \bmod q}$

UnSigncryption SECDSS1

Вход: d_B, Q_A, ш.т. c и подпись (r, s)
Выход: о.т. и результат проверки

1: Вычислить $u = sd_B$
2: Вычислить $\boxed{(k_1, k_2) = \mathrm{H}(uQ_A + urP)}$
3: Вычислить $m = D_{k_1}(c)$
4: **Если** $\mathrm{HK}_{k_2}(m) = r$ **то** принять m
5: **иначе** отвергнуть m

Заявляемые свойства

- **корректность** – расшифрование и проверка цифровой подписи может быть осуществлена только с использованием ключей, соответствующим ключам, использованным при зашифровании и формировании цифровой подписи.

Заявляемые свойства

- **корректность**
- **эффективность** – трудоемкость реализации должна быть «ниже», чем у совокупности независимых механизмов, используемых для решения аналогичной задачи конфиденциальной передачи информации с обеспечением свойства невозможности подделки подписи.

Заявляемые свойства

- **корректность**
- **эффективность**
- **безопасность** – механизм должен одновременно обеспечивать следующие основные свойства:
  - ☑ конфиденциальность;
  - ☑ аутентификация источника сообщения;
  - ☑ невозможность отказа от авторства;
  - ☑ целостность,

  а также дополнительные:
  - ☐ защищенность от чтения назад (forward secrecy);
  - ☐ **всеобщая** проверки корректности переданного сообщения.

Содержание

Возможность всеобщей верификации

Идея

Разделить ключи шифрования k_1 и «подписи» k_2

Signcryption Bao1998

Вход: d_A, Q_B и сообщение m
Выход: ш.т. c и подпись (r, s)

1: Выбрать $k \in_R \{1, 2, \ldots, q-1\}$
2: Вычислить $\boxed{k_1 = \mathrm{H}(kQ_B)}$
3: Вычислить $\boxed{k_2 = \mathrm{H}(kP)}$
4: Вычислить $c = E_{k_1}(m)$
5: Вычислить $r = \mathrm{HK}_{k_2}(m)$
6: Вычислить $s = k(r + d_A)^{-1} \bmod q$

UnSigncryption Bao1998

Вход: d_B, Q_A, ш.т. c и подпись (r, s)
Выход: о.т. и результат проверки

1: Вычислить $T_1 = s(Q_A + rP)$
2: Вычислить $T_2 = d_B T_1$
3: Вычислить $k_1 = \mathrm{H}(T_2)$
4: Вычислить $k_2 = \mathrm{H}(T_1)$
5: Вычислить $m = D_{k_1}(c)$
6: **Если** $\mathrm{HK}_{k_2}(m) = r$ **то** принять m
7: **иначе** отвергнуть m

F. Bao и R. Deng. A signcryption scheme with signature directly verifiable by public key. In: Proceedings of PKC 98, LNCS 1431, Springer-Verlag, 1998, pp. 55-59, 1998.

Защита от чтения назад

Напомним одну из формула для вычисления подписи

$s = k(r + d_A)^{-1} \bmod q$, где k основа ключа шифрования

Проблема

Если секретный ключ отправителя станет известным, то можно будет расшифровать все ранее созданные шифрсообщения

Y. Han, X. Yang и Y. Hu. Signcryption based on elliptic curve and its multi-party schemes. in Proceedings of the 3rd ACM International Conference on Information Security (InfoSecu 04), 2004.

Защита от чтения назад

Идея

Сделать так, чтобы по уравнению подписи нельзя было установить ключ шифрования, для этого добавить туда еще одну «неизвестную»

Signcryption Han2004

Вход: d_A, Q_B и сообщение m
Выход: ш.т. c и подпись (R, s)

1: Выбрать $r \in_R \{1, 2, \ldots, q-1\}$
2: Вычислить $R = rP = (x_1, y_1)$
3: Вычислить $K = rQ_B = (x_2, y_2)$
4: Вычислить $\boxed{s = r^{-1}(\mathrm{H}(m) + x_1 d_A) \bmod q}$
5: Вычислить $h = \mathrm{H}(m||s)$
6: Вычислить $c = (m \| h) \oplus x_2$

UnSigncryption Han2004

Вход: d_B, Q_A, ш.т. c и подпись (R, s)
Выход: о.т. и результат проверки

1: Вычислить $K = d_B R = (x_2', y_2')$
2: Вычислить $m' \| h' = c \oplus x_2'$
3: Вычислить $h'' = \mathrm{H}(m'||s)$
4: **Если** $h' = h''$ **то** продолжить
5: **иначе** отвергнуть m'
6: Вычислить $u = s^{-1}\mathrm{H}(m')$, $v = s^{-1}x_1$
7: Вычислить $(x_1', y_1') = uP + vQ_A$
8: **Если** $x_1 = x_1'$ **то** принять m'
9: **иначе** отвергнуть m'

Содержание

Плохой способ № 1

- в 2009 году предложен механизм, авторы которого заявляли возможность обеспечения всех свойств безопасности
- однако обоснования заявляемых свойств предложено не было

Signcryption Mohamed2009

Вход: d_A, Q_B и сообщение m
Выход: ш.т. c и подпись (R, s)

1: Выбрать $r \in_R \{1, 2, \ldots, q-1\}$
2: Вычислить $k_1 = \mathrm{H}(rP)$
3: Вычислить $k_2 = \mathrm{H}(rQ_B)$
4: Вычислить $c = E_{k_2}(m)$
5: Вычислить $h = \mathrm{H}(c, k_1)$
6: Вычислить $s = r(h + d_A)^{-1} \bmod q$
7: Вычислить $R = hP$

UnSigncryption Mohamed2009

Вход: d_B, Q_A, ш.т. c и подпись (R, s)
Выход: о.т. и результат проверки

1: Вычислить $k_1 = \mathrm{H}(s(R + Q_A))$
2: Вычислить $h = \mathrm{H}(c, k_1)$
3: Вычислить $k_2 = \mathrm{H}(d_B s(R + Q_A))$
4: Вычислить $m' = D_{k_2}(c)$
5: Вычислить $R' = hP$
6: **Если** $R' = R$ **то** принять m'
7: **иначе** отвергнуть m'

Плохой способ № 1

Недостатки механизма

- ✗ аутентификация передаваемого сообщения
  (аутентификация только зашифрованного сообщения)

Недостаток присущий всем Encrypt-then-Sign механизмам

- ✗ защита от чтения назад
  (защита не обеспечивается)

Вход: d_A известно нарушителю
1: Зная (R, s) и Q_A из равенства $k_1 = \mathrm{H}(s(R + Q_A))$ восстановить k_1
2: С использованием c и k_1 вычислить h
3: Из равенства $s = r(h + d_A)^{-1} \bmod q$ восстановить r
4: С использованием r и Q_B восстановить k_2
5: Расшифровать c

E. Mohamed и H. Elkamchouchi. Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy. International Journal of Computer Science and Network Security, vol. 9(1), pp. 395-398, 2009.

Плохой способ № 2

- в 2013 году предложен еще один механизм, авторы которого заявляли возможность обеспечения всех свойств безопасности
- однако обоснования заявляемых свойств предложено не было

Signcryption Amounas2013

Вход: d_A, Q_B и сообщение m
Выход: ш.т. c и подпись (R, S)

1: Выбрать точку $K = (x_K, y_K)$
2: Вычислить $c = E_{x_K}(m)$
3: Вычислить $r = \mathrm{H}(c, y_K)$
4: Вычислить $S = d_A r Q_B + K$
5: Вычислить $R = rQ_A$

UnSigncryption Amounas2013

Вход: d_B, Q_A, ш.т. c и подпись (R, S)
Выход: о.т. и результат проверки

1: Вычислить $S - d_B R = (x_K, y_K)$
2: Вычислить $r = \mathrm{H}(c, y_K)$
3: Вычислить $m' = D_{x_K}(c)$
4: Вычислить $R' = rQ_A$
5: **Если** $R' = R$ **то** принять m'
6: **иначе** отвергнуть m'

Плохой способ № 2

Недостатки механизма

✗ аутентификация источника сообщения

(любой пользователь B может создать сообщение, подпись под которым будет верифицирована с использованием ключа Q_A пользователя A, который не участвовал в процедуре формирования подписи)

Вход: B знает Q_A

1: Выбирает произвольную точку $K' = (x_{K'}, y_{K'})$

2: Для произвольного сообщения m вычисляет $c' = E_{x_{K'}}(m)$, $r' = \mathrm{H}(c', y_{K'})$

3: Вычисляет $S' = d_B r' Q_A + K' = d_B r' d_A P + K'$ и $R' = r' Q_A$.

4: Получает ш.т. c' и подпись (R', S') под ним

Выход: подпись под m может быть верифицирована с использованием Q_A

F. Amounas, H. Sadki и E. Kinani. An Efficient Signcryption Scheme based on The Elliptic Curve Discrete Logarithm Problem. International Journal of Information & Network Security, vol. 2(3), pp. 253-259, 2013.

Содержание

Можно ли применить методы анализа протоколов?

Заметим, что

signcryption-механизм представляет собой (однонаправленный/статический) протокол, где пользователь A, используя открытые параметры получателя B, направлет ему зашифрованное и подписанное сообщение

Рассмотрим атаку типа KCI

Что за тип? Нарушителю известен секретный ключ получателя и он хочет заставить получателя поверить в то, что тот получил корректное сообщение от пользователя, который в действительности не участвовал в его формировании

Зачем рассматривать? Подобный тип атак актуален, поскольку ранее исследования проводились в условиях, когда нарушителю известен секретный ключ отправителя

Применение к механизму SECDSS1

Вход: B известен d_C, A отправил m пользователю B
1: Вычислить $l = d_B d_C^{-1} \pmod q$
2: Положить $s' = ls \pmod q$
Выход: можно убедить C в том, что c и подпись (r, s') были созданы пользователем A и направлены C

Проверка

C должен вычислить значения

$$u = s'd_C = d_C lk(r + d_A)^{-1},$$
$$\mathrm{H}(uQ_A + urP) = \mathrm{H}(d_A d_C lk(r + d_A)^{-1}P + rd_C lk(r + d_A)^{-1}P) =$$
$$= \mathrm{H}(d_C lk(d_A + r)(r + d_A)^{-1}P) = \mathrm{H}(d_C lkP) = \mathrm{H}(kQ_B) = (k_1, k_2),$$

которые позволят ему вычислить $m = D_{k_1}(c)$ и проверить выполнение равенства $\mathrm{HK}_{k_2}(m) = r$

Содержание

Существует ли безопасный signcryption-механизм?

Идея

Добавить идентификаторы `id` отправителя и получателя

Signcryption Toorani2010

Вход: d_A, Q_B и сообщение m
Выход: ш.т. c и подпись (R, s)

1: Выбрать $r \in_R \{1, 2, \ldots, q-1\}$
2: Вычислить $R = rP = (x_R, y_R)$
3: Вычислить $(r + x_R d_A)Q_B = (x_K, y_K)$
4: Вычислить $k = \mathrm{H}(x_K, \mathtt{id}_A, y_K, \mathtt{id}_B)$
5: Вычислить $c = E_k(m)$
6: Вычислить $t = \mathrm{HK}_k(m, x_R, \mathtt{id}_A, y_R, \mathtt{id}_B)$
7: Вычислить $s = td_a - r \bmod q$

UnSigncryption Toorani2010

Вход: d_B, Q_A, ш.т. c и подпись (R, s)
Выход: о.т. и результат проверки

1: Вычислить $d_B(R + x_R Q_A) = (x_K, y_K)$
2: Вычислить $k = \mathrm{H}(x_K, \mathtt{id}_A, y_K, \mathtt{id}_B)$
3: Вычислить $m' = D_k(c)$
4: Вычислить $t = \mathrm{HK}_k(m', x_R, \mathtt{id}_A, y_R, \mathtt{id}_B)$
5: **Если** $sP + R = tQ_A$ **то** принять m'
6: **иначе** отвергнуть m'

M. Toorani и A. Shirazi. An elliptic curve-based signcryption scheme with forward secrecy. Journal of Applied Sciences, vol. 9 (6), pp. 1025-1035, 2010.

Содержание

Основные выводы

- возможность проверки корректности полученного сообщения без использования секретного ключа получателя
  - ☑ «разделение» ключей, применяемых для зашифрования и формирования цифровой подписи
- защита от чтения назад
  - ☑ использование такого уравнения подписи, где добавлена еще одна «переменная»
- защита от KCI-атаки
  - ☑ использование информации об абонентах

Спасибо за внимание