УДК 681.3.06

АНАЛІЗ ЗАХИЩЕНОСТІ АЛГОРИТМУ ЦИФРОВОГО ПІДПИСУ EC KCDSA ВІД АТАК НА ЗВ'ЯЗАНИХ КЛЮЧАХ

О. С. АКОЛЬЗІНА, І. Д. ГОРБЕНКО

Розглядаються сутність, умови та можливості здійснення порушниками атак з метою підробки електронних підписів на основі зв'язування особистих ключів електронного підпису, наводяться рекомендації відносно забезпечення захисту від атак на основі зв'язування особистих ключів.

Ключові слова: алгоритм електронного підпису згідно з ДСТУ ISO/IEC 14888-3:2014, атака на основі зв'язування ключів, особисті сеансові та довгострокові ключі.

ВСТУП

Алгоритм електронного підпису (ЕП) EC KCDSA вважається одним з найбільш надійних криптографічних алгоритмів ЕП на світовому рівні, він також реалізований у національному стандарті ДСТУ ISO/IEC 14888-3. Вказаний стандарт введено в Україні в дію наказом Мінекономрозвитку №1493 з 1 січня 2016 року. Незважаючи на його рівень стандартизації, існує необхідність детального вивчення його на предмет криптографічної стійкості від існуючих та потенційних атак.

Метою цієї статті і є аналіз захищеності алгоритму електронного підпису EC KCDSA від атак на зв'язаних ключах та розробка рекомендацій відносно протидії їм.

1. СУТНІСТЬ, ПРИЗНАЧЕННЯ ТА ОСНОВИ ЗАСТОСУВАННЯ EC KCDSA

Алгоритм EC KCDSA – це алгоритм, що розроблений командою Korea Internet & Security Agency, він є дещо аналогом алгоритму KCDSA, але на еліптичних кривих. В алгоритмі реалізується механізм вироблення ЕП з додатком (доповненням) [1, 2]. Цей алгоритм відкликано з [1] та введено в [2].

ЕП повідомлення M згідно з EC KCDSA, що виробляється підписувачем, складається з двох складових – цілих чисел r та s, обчислених за модулем простого числа – порядку базової точки.

В процесі підписування повідомлення M згідно з EC KCDSA підписувач виконує такі кроки:

1. Обчислюється геш-значення повідомлення M та даних сертифіката z_A, тобто

$$e = h(z_A \| M).$$

2. Генерується (вибирається) випадкове ціле число – ключ сеансу k.

3. Обчислюється геш-значення

$$r = h(\pi(kG)) = h(c),$$

де π є функцією, що виділяє x – координату точки kG та перетворює її у рядок байтів і присвоює йому значення змінної c, а також обчислюється геш-значення $h(c)$.

4. Здійснюється зв'язування значення r та геш-значення e у вигляді $w = r \, XOR \, e$.

5. З використанням особистого ключа d, таємного ключа сеансу k та значення w обчислюється значення ЕП s за модулем порядку базової точки n:

$$s = d(k - w) \bmod q. \quad (1)$$

На останок до повідомлення M додається значення ЕП – (r, s).

Перевіряння ЕП повідомлення M', наприклад, об'єкта A об'єктом B, здійснюється у такій послідовності:

1. Перевіряється виконання умов, що $0 < s' < n$ та $len_{r'} \le len_{h()}$, якщо хоч одна умова не виконується, тоді повідомлення відхиляється.

2. Обчислюється геш-значення

$$e' = h(z_A \| M').$$

3. Обчислюється значення $w' = r' \, XOR \, e'$.

4. Обчислюється значення точки еліптичної кривої у вигляді

$$(x_1', y_1') = s'Q_A + w'G. \quad (2)$$

5. Виділяється та перетворюється значення координати x_1' в рядок байтів, якому присвоюється значення c.

6. Обчислюється геш-значення $v = h(c)$.

Якщо $r' = v$, тоді ЕП і відповідно повідомлення М приймаються перевірником як справжні та цілісні, інакше – відхиляється.

Примітка. Якщо використовують несправжнє значення відкритого ключа Q або несправжнє значення Z_A, тоді процес перевіряння ЕП повідомлення M буде з великою ймовірністю невдалим.

2. СТІЙКІСТЬ АЛГОРИТМУ ДО ОСНОВНИХ ВИДІВ АТАК

Основною вимогою до ЕП є забезпечення криптографічної стійкості проти усіх відомих та потенційних атак, причому складність має носити експоненційний характер [2, 3, 5–7].

На сьогодні існує значне число атак на ЕП, достатньо детально вони описані та аналізуються в [5–7].

Як правило, атаки реалізуються в процесі здійснення криптоаналізу. При здійсненні криптоаналізу вважається, що криптоаналітику відомі методи, алгоритми й протоколи ЕП, загально-системні параметри та відкриті ключі. Вважається також, що криптоаналітик володіє усім необхідним програмним та апаратним забезпеченням ЕП, невідомим є тільки особистий ключ. Додатково може бути відомий інтервал

або клас, якому належить особистий ключ, вага Хеммінга ключа, або його ймовірнісний розподіл. Звичайно ці відомості спрощують задачу знаходження дискретного логарифма.

Доведено [1–3, 5–6], що агоритм ЕП ЕС KCDSA захищений від таких типів атак, як: «повне розкриття», на основі підписаних даних, «екзистенційна підробка», «селективна підробка». Така захищеність забезпечується, в тому числі, за рахунок обов'язкового використання колізійно-стійких функцій гешування [4–5].

Також обов'язковими умовами забезпечення криптографічної захищеності від атак є забезпечення конфіденційності, цілісності, справжності (автентичності), доступності, надійності та неспростовності особистого ключа. Відносно відкритого ключа не вимагається забезпечення його конфіденційності, обов'язково відносно нього мають забезпечуватися цілісність, справжність (автентичність), доступність, та неспростовність.

Зазначені послуги, як правило, забезпечуються засобом захищеного генерування особисто власником (підписувачем) асиметричних пар ключів, безпечним зберіганням та застосуванням особистого ключа, виготовленням та обслуговуванням сертифікатів відкритих ключів у третьої довіреної сторони, як правило в центрі сертифікації ключів відповідної інфраструктури відкритого ключа [2–4].

До цих пір у доступних джерелах вважалось [1, 5–6], що ЕП ЕС KCDSA захищений від атаки на зв'язаних ключах. Наші дослідження показали, що атака вказаного ЕП на зв'язаних ключах існує і є критичною за певних умов для підписувача. Тому розглянемо це питання детально.

3. СУТНІСТЬ ТА УМОВИ ЗДІЙСНЕННЯ АТАКИ НА ЗВ'ЯЗАНИХ СЕАНСОВИХ КЛЮЧАХ

При атаці на зв'язаних ключах, на відміну від інших атак, порушник певним чином може мати доступ до ключа сеансу чи довгострокового особистого ключа, наприклад, за рахунок влаштування спеціальних лазівок у програмне чи програмно-апаратне забезпечення, яке використовується в ході вироблення ЕП.

У подальшому вважатимемо, що порушником є криптоаналітик третього рівня [5–6], який під час виконання криптоаналізу може спиратися на науково-технічний ресурс, що прирівнюється до науково-технічного ресурсу спецслужби економічно розвиненої держави.

Розглянемо санкціонованого користувача, який здійснює такі зловмисні дії. Робиться спроба для інформації (повідомлень) M_i та M_j виробити однакові ЕП. Якщо це буде зроблено, то далі зловмисник може маніпулювати цими підписаними повідомленнями, висуваючи або передаючи в ході реалізації загроз те чи інше повідомлення, але обидва вони прийматимуться отримувачем як справжні та цілісні з правильним підписом [5–6].

Нехай зв'язаними є ключі k_1 та k_2 сеансів, тобто які мають змінюватися при кожному виробленні ЕП. В ході аналізу вважатимемо, що особистий ключ d_a є дійсним протягом деякого часу ΔT, а k_1 і k_2 є зв'язаними ключами відповідних сеансів ЕП, причому $k_1 + k_2 = n$. В цьому випадку $k_2 = n - k_1$. Результати аналізу вироблення підписів для повідомлень M_i та M_j наведені в табл. 1.

Аналіз даних табл. 1 показує, що відкриті сеансові ключі r_1 та r_2 в алгоритмі ЕП ЕС KCDSA в ході застосування їх для підпису різних повідомлень M_i та M_j зв'язаних ключів, співпадають. Вказане є значним недоліком алгоритму ЕП ЕС KCDSA. Але на кроці 6 ми отримуємо, що з великою ймовірністю $w_1 \neq w_2$, оскільки геш-функція, що застосовується в алгоритмі вироблення ЕП, є колізійно стійкою.

Надалі розглянемо, чи існує можливість, за якої для різних повідомлень M_i та M_j співпадатимуть самі підписи s_1 та s_2 та яка ймовірність такої події. Тобто визначимо умови, за яких компоненти s_1 та s_2 ЕП ЕС KCDSA для двох довільних різних повідомлень M_i та M_j, співпадуть. Для цього прирівняємо праві частини s_1 та s_2 сьомих рядків табл. 1. В результаті маємо.

$$d_a(k_1 - w_1) \bmod n = d_a(k_2 - w_2) \bmod n \qquad (3)$$

або

$$(k_1 - w_1) \bmod n = (n - k_1 - w_2) \bmod n = \\ = -(k_1 + w_2) \bmod n. \qquad (4)$$

Далі отримаємо, що:

$$2k_1 = (w_1 - w_2) \bmod n$$

або

$$k_1 = \frac{w_1 - w_2}{2} \bmod n = \frac{r_1 \oplus h_1 - r_2 \oplus h_2}{2} \bmod n. \qquad (5)$$

Аналіз співвідношень (4) та (5) щодо захищеності ЕС KCDSA дозволяє зробити такі висновки.

Таблиця 1

Алгоритм вироблення ЕП для ЕС-КС DSA зі зв'язаними сеансовими ключами

Для повідомлення M_i	Для повідомлення M_j
1. $h_1 = H(Z_a \parallel M_1)$	1. $h_2 = H(Z_a \parallel M_2)$
2. $k_1 \in [1, n-1]$	2. $k_2 = n - k_1, k_2 \in [1, n-1]$
3. $(x_1, y_1) = k_1 G$	3. $(x_2, y_2) = k_2 G = (n - k_1)G = nG(\bmod n) - k_1 G(\bmod n) = 0 - k_1 G(\bmod n) = (x_1, -y_1)$
4. $x_1 \to c_1$	4. $x_2 = \pi(x_1, -y_1) = x_1 \to c_2 = c_1$
5. $r_1 = H(c_1)$	5. $r_2 = H(c_2) = H(c_1) = r_1$
6. $w_1 = r_1 \oplus h_1$	6. $w_2 = r_1 \oplus h_2$
7. $s_1 = d_1(\mathrm{k}_1 - w_1) \bmod n$	7. $s_2 = d_2(\mathrm{k}_2 - w_2) \bmod n$

1. Значення відкритих сеансових ключів r_1 та r_2 відповідно для k_1 та $k_2 = n = k_1$ особистих сеансових ключів співпадають, незалежно від повідомлень M_i та M_j, які підписуються. Це безпосередньо випливає з третього і п'ятого рядків табл. 1.

2. Співвідношення (5) вказує на умову здійснення атаки на зв'язаних ключах. Для здійснення атаки необхідно обчислити k_1 згідно з (5). Це можна зробити, оскільки r_1 порушнику відоме, а геш-значення повідомлень $h_1(M_1)$ та $h_2(\mathrm{M}_2)$ він може обчислити.

3. Таким чином, алгоритм ЕП ЕС KCDSA незахищений від атаки на зв'язаних сеансових ключах, а співвідношення (5) визначає умову підробки підпису для повідомлення M_j при відомих даних відносно.

4. Для захисту алгоритму ЕП ЕС KCDSA від атаки на зв'язаних сеансових ключах необхідно виключити можливість зв'язування сеансових ключів у процесі підписування повідомлень. Основним підходом до забезпечення вищезазначеного є практичне виключення можливостей запису викривленого програмного забезпечення, що дозволяє зв'язувати сеансові ключі, наприклад, засобом використання апаратно-програмних чи апаратних засобів криптографічних перетворень під час підписування повідомлень.

4. СУТНІСТЬ ТА УМОВИ ЗДІЙСНЕННЯ АТАКИ НА ДОВГОСТРОКОВИХ ЗВ'ЯЗАНИХ КЛЮЧАХ

Розглянемо також можливість та умови здійснення засобом зв'язування довгострокових ключів. Таке зв'язування може бути здійснене на етапах генерування асиметричних пар ключів ЕП.

Нехай зв'язування довгострокових ключів здійснюється таким чином

$$d_2 = n - d_1,\ k_1 = k_2 = k. \qquad (6)$$

У табл. 2 наведений алгоритм вироблення ЕП для EC-KCDSA на довгострокових зв'язаних ключах.

Далі, використовуючи сьомі рядки табл. 2, визначимо умову співпадання інших складових ЕП s_1 та s_2 для зв'язаних довгострокових ключів, наприклад коли $s_1 = s_2$. В результаті маємо, що

$$d_1(k - w_1) = -d_1(k - w_2) \bmod n;$$
$$k - w_1 = -k - w_2 (\bmod n);$$
$$k = (w_1 - w_2)/2 (\bmod n). \qquad (7)$$

На основі аналізу (6) можна зробити висновок, що при зв'язуванні довгострокових ключів за правилом (6) не вдається визначити умову, за якої – $s_1 = s_2$. Тому модифікуємо залежність між довгостроковими ключами таким чином

$$d_2 = n - d_1 \pm 1. \qquad (8)$$

Нехай знову виконується рівність $k_1 = k_2 = k$.

У табл. 3 наведений алгоритм вироблення ЕП для ЕС KCDSA на довгострокових зв'язаних ключах згідно з (8).

Визначимо умову вироблення однакових s – компонент ЕП, тобто: прирівняємо праві частини сьомого рядка табл. 3. В результаті отримуємо

$$d_1(k - w_1) \bmod n =$$
$$= (-d_1 \pm 1)(k - w_2) d_1 (k - w_1) \bmod n = \qquad (9)$$
$$= (-d_1 \pm 1)(k - w_2)$$

або

$$\frac{k - w_1}{k - w_2} = \frac{-d_1 \pm 1}{d_1} (\bmod n).$$

Таблиця 2

Алгоритм вироблення ЕП для EC-KCDSA на довгострокових зв'язаних ключах

Для повідомлення M_i	Для повідомлення M_j
1. $h_1 = H(Z_a \parallel M_1)$	1. $h_2 = H(Z_a \parallel M_2)$
2. $k \in [1, n-1]$	2. $k \in [1, n-1]$
3. $(x_1, y_1) = kG$	3. $(x_2, y_2) = kG = (x_1, y_1)$
4. $x_1 \to c_1$	4. $x_2 = \pi(x_1, y_1) = x_1 \to c_2 = c_1$
5. $r_1 = H(c_1)$	5. $r_2 = H(c_2) = H(c_1) = r_1$
6. $w_1 = r_1 \oplus h_1$	6. $w_2 = r_1 \oplus h_2$
7. $s_1 = d_1(k - w_1) \bmod n$	7. $s_2 = d_2(k - w_2) \bmod n = (n - d_1)(k - w_2) \bmod n = -d_1(k - w_2) \bmod n$

Таблиця 3

Алгоритм вироблення ЕП для EC-KCDSA зі зв'язаними довгостроковими ключами згідно з (8)

Для повідомлення M_i	Для повідомлення M_j
1. $h_1 = H(Z_a \parallel M_1)$	1. $h_2 = H(Z_a \parallel M_2)$
2. $k \in [1, n-1]$	2. $k \in [1, n-1]$
3. $(x_1, y_1) = kG$	3. $(x_2, y_2) = kG = (x_1, y_1)$
4. $x_1 \to c_1$	4. $x_2 = \pi(x_1, y_1) = x_1 \to c_2 = c_1$
5. $r_1 = H(c_1)$	5. $r_2 = H(c_2) = H(c_1) = r_1$
6. $w_1 = r_1 \oplus h_1$	6. $w_2 = r_1 \oplus h_2$
7. $s_1 = d_1(k - w_1) \bmod n$	7. $s_2 = d_2(k - w_2) \bmod n = (n - d_1 \pm 1)(k - w_2) \bmod n = (-d_1 \pm 1)(k - w_2) \bmod n$

Далі отримуємо, що

$$\frac{k-w_1}{k-w_2}=\pm\frac{1}{d_1}-1(\mathrm{mod}n)$$

$$\pm d_1=\frac{k-w_2}{2k-w_1-w_2}(\mathrm{mod}n) \qquad (10)$$

та

$$d_1=\mp\frac{k-w_2}{2k-w_1-w_2}(\mathrm{mod}n) \qquad (11)$$

при варіантах зв'язування

$$d_2=n-d_1+1(\mathrm{mod}n)d_2=n-d_1+1(\mathrm{mod}n)$$

та $d_2=n-d_1-1(\mathrm{mod}n)d_2=n-d_1-1$.

Вираз (11) визначає умову співпадання ЕП при зв'язуванні довгострокових ключів. Якщо враховувати, що термін дії довгострокового ключа щонайменше один рік, то порушник зможе використати зв'язані довгострокові ключі лише один раз. Цього буде достатньо для здійснення підробки.

Отже, якщо буде здійснене зв'язування довгострокових ключів у розглянутий спосіб, то він досягне своєї мети – обидві компоненти підпису (r, s) для різних повідомлень M_1 та M_2 співпадуть, що дозволить підробити ЕП

5. СУТНІСТЬ ТА УМОВИ ЗДІЙСНЕННЯ АТАКИ НА ЗВ'ЯЗАНИХ ДОВГОСТРОКОВИХ ТА СЕАНСОВИХ КЛЮЧАХ

Розглянемо можливість здійснення атаки на основі поєднання двох попередніх атак – зв'язування як довгострокових, так і короткострокових ключів. У цьому випадку не потрібно, щоб $k_1=k_2=k$.

Нехай короткострокові ключі виробляються з порушенням порушником у такий спосіб:

$$k_2=n-k_1 \bmod n, \qquad (12)$$

а довгострокові таким чином:

$$d_2=n-d_1\pm1. \qquad (13)$$

Алгоритм вироблення ЕП при зв'язуванні довгострокових та короткострокових ключів наведений у табл. 4.

Визначимо умову співпадіння s_1 та s_2: прирівнявши праві частини(7) табл. 4.

$$d_1(k_1-w_1)=(-d_1\pm1)(-k_1-w_2)\bmod n; \qquad (14)$$

або

$$\frac{k_1-w_1}{-k_1-w_2}=\frac{-d_1\pm1}{d_1}(\mathrm{mod}n),$$

$$\frac{k_1-w_1}{-k_1-w_2}=\pm\frac{1}{d_1}-1(\mathrm{mod}n),$$

оскільки порушнику відомі k_1, w_1 та w_2, то він може обчислити

$$\pm d_1=\frac{-w_1-w_2}{k_1-w_2}(\mathrm{mod}n) \qquad (15)$$

або

$$d_1=\pm\frac{w_1+w_2}{k_1-w_2}(\mathrm{mod}n). \qquad (16)$$

Зробимо уточнення відносно реалізації атак зі зв'язуванням довгострокових ключів. Так аналіз (10), (11), (15) та (16) показує, що довгостроковий ключ d_1 та сенсовий k_1 можуть бути розраховані тільки під час вироблення ЕП, оскільки значення w_1 та w_2 залежать від самих повідомлень M_i, M_j і обчислюються у процесі підпису. При цьому для реалізації атаки порушник повинен закласти в систему генерування асиметричних пар ключів відповідну закладку, яка дозволяла б у певний момент здійснити зв'язування довгострокових та короткострокових ключів (або встановити однакові короткострокові ключів).

6. ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

1. Проведені дослідження алгоритму ЕП EC-KCDSA, що входить в ДСТУ ISO/IEC 14888-3:2014, та отримані результати дозволяють зробити висновки про те, що відносно нього існують ефективні атаки підробки ЕП, які грунтуються на зв'язуванні особистих ключів. Також у процесі досліджень отримано нові умови зв'язування особистих ключів та комбінацій сеансових та довгострокових ключів.

2. Одним з найбільш ефективних методів захисту від атак на зв'язаних ключах є використання криптографічних протоколів та надійних апаратно-програмних чи апаратних засобів ЕП, для яких практично не можливо зв'язування ключів.

3. Значно ускладнюється можливість здійснення атаки зв'язування ключів засобом використання в процесі вироблення ЕП геш-значення різних констант, наприклад, залежних від параметрів криптографічних перетворень.

Таблиця 4

Алгоритм вироблення ЕП для EC-KCDSA зі зв'язаними довгостроковими та сеансовими ключами

Для повідомлення M_i	Для повідомлення M_j
1. $h_1=H(Z_a \parallel M_1)$	1. $h_2=H(Z_a \parallel M_2)$
2. $k_1\in[1,n-1]$	2. $k_2=n-k_1 \bmod n$
3. $(x_1,y_1)=kG$	3. $(x_2,y_2)=-k_1G=(x_1,-y_1)=(x_1,\mathrm{y}_1)$
4. $x_1\to c_1$	4. $x_2=\pi(x_1,y_1)=x_1\to c_2=c_1$
5. $r_1=H(c_1)$	5. $r_2=H(c_2)=H(c_1)=r_1$
6. $w_1=r_1\oplus h_1$	6. $w_1=r_2\oplus h_2=r_1\oplus h_2$
7. $s_1=d_1(k-w_1)\bmod n$	7. $s_2=d_2(k-w_2)\bmod n=(n-d_1\pm1)(-k_1-w_2)\bmod n=(-d_1\pm1)(-k_1-w_2)\bmod n$

4. При спробах підробки ЕП відносно алгоритму ЕП EC-KCDSA, що входить в ДСТУ ISO/IEC 14888-3:2014, для порушника більш раціональним є здійснення атаки на основі зв'язування сеансових ключів, тому необхідно в першу чергу здійснювати захист від таких дій порушників.

Література

[1] ISO/IEC 15946-2:2002, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signatures.

[2] ISO/IEC 14888-3:2006 Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms.

[3] ДСТУ ISO/IEC 14888-3:2014 (проект) «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. – Частина 3: Механізми на основі сертифікатів» [на заміну ДСТУ ISO/IEC 14888-3:2002].

[4] ISO/IEC 10118-3. Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions.

[5] *Горбенко І.Д., Горбенко Ю.І.* Прикладна криптологія. Теорія. Практика. Застосування. // Монографія. Видання 2-ге, перероблене й виправлене. – Харків. Видавництво «ФОРТ», 2012. – 878 с.

[6] *Горбенко Ю.І.* Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації. Монографія. – Харків. Форт. 2015. – 959 с.

[7] *Акользіна О.С, Бакликов О.О.* Порівняльний аналіз перспективних стандартів ЕП в групі точок еліптичних кривих // Радіотехніка. – 2015. – 181. – С. 101–109.

Надійшла до редколегії 17.11.2015

Акользіна Ольга Сергіївна, фото та відомості про автора див. на стор. 290.

Горбенко Іван Дмитрович, професор, доктор технічних наук, лауреат державної премії в галузі науки і техніки, головний конструктор ПАТ «ІІТ». Наукові інтереси: криптологія та кібербезпека.

УДК 681.3.06

Анализ защищенности алгоритма цифровой подписи EC-KCDSA от атак на связанных ключах / О.С. Акользина, И.Д. Горбенко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2015. – Том 14. – № 4. – С. 291–295.

Приводятся результаты анализа защищенности алгоритма ЦП EC-KCDSA от атак на связанных ключах. Разработаны варианты атак на связанных долгосрочных ключах.

Даются рекомендации по применению данного алгоритма.

Ключевые слова: цифровая подпись, EC-KCDSA, атака на связанных ключах.

Табл.: 4. Библиогр.: 7 назв.

UDC 681.3.06

Analysis of EC-KCDSA electronic signature algorithm protectability from key-related atacks / O.S. Akolzina, I.D. Gorbenko // Applied Radio Electronics: Sci. Journ. — 2015. — Vol. 14. — № 4. — P. 291–295.

The results of analyzing the EC-KCDSA electronic signature algorithm protectability from key-related attacks are provided. Some methods of long-time related key attacks have been developed. Application recommendations of the said algorithm are given.

Keywords: electronic signature, EC-KCDSA, key-related attack.

Tab.: 4. Ref.: 7 items.