НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

Інформаційні технології

МЕТОДИ ЗАХИСТУ ЦИФРОВІ ПІДПИСИ З ДОПОВНЕННЯМ

Частина 1. Загальні положення (ISO/IEC 14888-1:1998, IDT)

ДСТУ ISO/IEC 14888-1:2002

Видання офіційне

Київ
ДЕРЖСПОЖИВСТАНДАРТ УКРАЇНИ
2006

БЗ № 3–2002/186

ПЕРЕДМОВА

1 ВНЕСЕНО: Технічний комітет стандартизації «Інформаційні технології» (ТК 20) при Держспоживстандарті України; Міжнародний науково-навчальний центр інформаційних технологій і систем НАН України та Міністерства освіти і науки України

ПЕРЕКЛАД І НАУКОВО-ТЕХНІЧНЕ РЕДАГУВАННЯ: **А. Анісімов,** д-р фіз.-мат. наук; **В. Задірака,** д-р фіз.-мат. наук; **О. Олексюк,** д-р екон. наук; **Є. Осадчий,** канд. техн. наук; **М. Афанасенко; Л. Данильченко; Т. Кальчук; В. Осадчий; В. Ткаченко; В. Чорноморець**

2 НАДАНО ЧИННОСТІ: наказ Держстандарту України від 12 липня 2002 р. № 422, зі зміною дати чинності згідно з наказом № 273 від 27 вересня 2005 р.

3 Національний стандарт відповідає ISO/IEC 14888-1:1998 Information technology — Security techniques — Digital signatures with appendix — Part 1: General (Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення)

Ступінь відповідності — ідентичний (IDT)

Переклад з англійської (en)

4 УВЕДЕНО ВПЕРШЕ

ЗМІСТ

НАЦІОНАЛЬНИЙ ВСТУП

Цей стандарт є тотожний переклад ISO/IEC 14888-1:1998 Information technology — Security techniques — Digital signatures with appendix — Part 1: General (Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення).

Відповідальний за міжнародний стандарт ISO/IEC 14888-1:1998 є Технічний комітет ISO/IEC JTC 1.

Відповідальний за цей стандарт в Україні — Технічний комітет стандартизації «Інформаційні технології» (ТК 20).

Структура ДСТУ ISO/IEC 14888 відповідає структурі міжнародного стандарту ISO/IEC 14888 і складається з таких частин:

ДСТУ ISO/IEC 14888-1:2002 Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення;

ДСТУ ISO/IEC 14888-2:2002 Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми на основі ідентифікаторів;

ДСТУ ISO/IEC 14888-3:2002 Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі сертифікатів.

У цьому стандарті наведено загальні принципи та вимоги до цифрових підписів із доповненням. Ця частина містить визначення та символи, спільні для всіх частин ДСТУ ISO/IEC 14888.

До стандарту внесено такі редакційні зміни:

— замінено слова «ISO/IEC 14888» та «ця частина ISO/IEC 14888» на слова «цей стандарт» та «ця частина стандарту» відповідно;

— у розділі «Нормативні посилання» надано переклад назв стандартів українською мовою.

Треба взяти до уваги, що в Україні чинний ДСТУ ISO/IEC 11770-3:2002 «Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми із застосуванням асиметричних методів». Ступінь відповідності міжнародному стандарту — ідентичний (IDT).

З міжнародними стандартами, на які є пóсилки в цій частині стандарту, можна ознайомитися в Головному фонді нормативних документів ДП «УкрНДНЦ».

НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

МЕТОДИ ЗАХИСТУ
ЦИФРОВІ ПІДПИСИ З ДОПОВНЕННЯМ

Частина 1. Загальні положення

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

МЕТОДЫ ЗАЩИТЫ
ЦИФРОВЫЕ ПОДПИСИ С ДОПОЛНЕНИЕМ

Часть 1. Общие положения

INFORMATION TECHNOLOGY

SECURITY TECHNIQUES
DIGITAL SIGNATURES WITH APPENDIX

Part 1. General

Чинний від 2006–10–01

1 СФЕРА ЗАСТОСУВАННЯ

Цей стандарт визначає кілька механізмів цифрових підписів з доповненням для повідомлень довільної довжини.

Ця частина стандарту містить загальні принципи і вимоги для цифрових підписів з доповненням. Вона також містить визначення і символи, спільні для всіх частин цього стандарту.

2 НОРМАТИВНІ ПОСИЛАННЯ

Наведені нижче нормативні документи містять положення, які через по́силки в цьому тексті становлять положення цієї частини стандарту. У разі датованих по́силок пізніші зміни до будь-якого з цих видань або перегляд їх не застосовують. Однак учасників угод, що ґрунтуються на цьому стандарті, запрошують визначити можливість застосування найостанніших видань нормативних документів, наведених нижче. У разі недатованих по́силок радять звертатися до найновішого видання нормативних документів. Члени IEC та ISO впорядковують каталоги чинних міжнародних стандартів.

У цьому стандарті є по́силки на такі стандарти:

ISO/IEC 9796:1991 Information technology — Security techniques — Digital signature scheme giving message recovery

ISO/IEC 9796-2:1997 Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Mechanisms using a hash-function

ISO/IEC 10118-1:1994 Information technology — Security techniques — Hash functions — Part 1: General

ISO/IEC 11770-3:1999 Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques.

Видання офіційне

★

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

ISO/IEC 9796:1991 Інформаційні технології. Методи захисту. Схема цифрового підпису, що відновлює повідомлення

ISO/IEC 9796-2:1997 Інформаційні технології. Методи захисту. Схема цифрового підпису, що відновлює повідомлення. Частина 2. Механізми, що використовують геш-функцію

ISO/IEC 10118-1:1994 Інформаційні технології. Методи захисту. Геш-функції. Частина 1. Загальні положення

ISO/IEC 11770-3:1999 Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми із застосуванням асиметричних методів.

В Україні чинний ДСТУ ISO/IEC 11770-3:2002 Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми із застосуванням асиметричних методів (ISO/IEC 11770-3:1996, IDT).

3 ЗАГАЛЬНІ ПОЛОЖЕННЯ

Механізми, зазначені в цьому стандарті, засновані на методах асиметричної криптографії. Кожен асиметричний механізм цифрового підписування містить три основних етапи:

— процес генерування пар ключів, де кожна пара складається з ключа підпису і відповідного перевіркового ключа;

— процес, що використовує ключ підпису і називається процесом підписування;

— процес, що використовує перевірковий ключ і називається процесом перевіряння підпису.

Перевіряння цифрового підпису потребує перевіркового ключа особи, що ставить підпис (підписувача). Для особи, що перевіряє підпис (перевірювача), таким чином, суттєво мати можливість зв'язати цей правильний перевірковий ключ з підписувачем, чи, точніше, з його ідентифікаційними даними (з їхньою частиною).

Якщо такий зв'язок так чи інакше властивий самому перевірковому ключу безпосередньо, то говорять, що схема «заснована на ідентифікаторах». Інакше зв'язок правильного перевіркового ключа з даними ідентифікації підписувача треба забезпечувати іншими засобами. Якою б не була природа таких засобів, схема тоді вважається «заснованою на сертифікатах».

Процедури підтверджування перевіркових ключів і керування ними в схемі, заснованій на сертифікатах, не є предметом розгляду цього стандарту. Механізми розподіляння відкритих перевіркових ключів розглядаються в ISO/IEC 11770-3.

4 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У цьому стандарті застосовуються такі терміни і визначення.

4.1 доповнення (*appendix*)
Рядок бітів, сформований з підпису і деякого довільного тексту

4.2 призначення (*assignment*)
Елемент даних, що є функцією свідоцтва і, можливо, частини повідомлення, який формує частину входу для функції підпису

4.3 геш-функція, стійка до колізій (*collision resistant hash-function*)
Геш-функція (див. ISO/IEC 10118-1), що має таку властивість: щодо обчислювання неможливо знайти будь-які два різні входи, які перетворюються в той самий вихід.

Примітка. Можливість обчислення залежить від специфічних вимог безпеки та оточення

4.4 детермінований (*deterministic*)
Незалежний від рандомізатора, нерандомізований

4.5 цифровий підпис (*digital signature*)
Див. підпис

4.6 параметр проблемної області (*domain parameter*)
Елемент даних, що є загальним і відомим (чи доступним) для всіх об'єктів у межах певної проблемної області

4.7 геш-код (*hash-code*)
Рядок бітів, що є виходом геш-функції

4.8 геш-функція (*hash-function*)
Функція (див. ISO/IEC 10118-1), що перетворює рядок бітів у рядок бітів зафіксованої довжини і має такі дві властивості:
— для певного виходу щодо обчислювання неможливо знайти вхід, що перетвориться в цей вихід;
— для певного входу щодо обчислювання неможливо знайти другий вхід, що перетвориться в той самий вихід.

Примітка. Можливість обчислення залежить від специфічних вимог безпеки та оточення

4.9 геш-атрибут (*hash-token*)
Зчеплення геш-коду й довільного контрольного поля, яке зветься ідентифікатором геш-функції, яке можна використовувати для ідентифікації геш-функції та методу доповнення

4.10 дані ідентифікування (*identification data*)
Послідовність елементів даних, охоплюючи індивідуальний ідентифікатор об'єкта, передаваних йому та використовуваних для його ідентифікування.

Примітка. Дані ідентифікування можуть додатково містити такі елементи даних, як ідентифікатор процесу підписування, ідентифікатор ключа підпису, період законності ключа підпису, обмеження на використання ключа, параметри, зв'язані з політикою безпеки, серійний номер ключа чи параметри проблемної області

4.11 повідомлення (*message*)
Рядок бітів довільної довжини

4.12 попередній підпис; передпідпис (*pre-signature*)
Значення, обчислене у процесі підписування, що є функцією рандомізатора і не залежить від повідомлення

4.13 рандомізований (*randomized*)
Залежний від рандомізатора

4.14 рандомізатор (*randomizer*)
Секретний елемент даних, створений підписувачем у процесі попереднього підписування, який не може бути передбачений іншими об'єктами

4.15 підпис (*signature*)
Рядок бітів (див. ISO/IEC 9796), який є результатом процесу підписування.

Примітка. Цей рядок бітів може мати внутрішню структуру, специфічну стосовно механізму підписування

4.16 рівняння підпису (*signature equation*)
Рівняння, яке визначає функцію підпису

4.17 функція підпису (*signature function*)
Функція процесу підписування, яка залежить від ключа підпису і параметрів проблемної області. Функція підпису має на вході призначення і, можливо, рандомізатор і видає на виході другу частину підпису

4.18 ключ підпису (*signature key*)
Секретний елемент даних, який стосується об'єкта і вживається тільки цим об'єктом у процесі підписування

4.19 процес підписування; підписування (*signature process*)
Процес, що отримує на вході повідомлення, ключ підпису і параметри проблемної області та видає на виході підпис

4.20 підписане повідомлення (*signed message*)
Набір елементів даних, що складається з підпису, тієї частини повідомлення, яку неможливо відновити з підпису, і довільного тексту.

Примітка. У контексті цього стандарту повне повідомлення включене в підписане повідомлення, і немає такої частини повідомлення, що не відновлюється з підпису

4.21 перевіркова функція (*verification function*)
Функція, що бере участь у процесі перевіряння, яка залежить від перевіркового ключа і на виході дає повторно обчислене значення свідоцтва

4.22 перевірковий ключ (*verification key*)
Елемент даних, що математично зв'язаний з ключем підпису об'єкта і якого використовує перевірювач у процесі перевіряння

4.23 процес перевіряння; перевіряння (*verification process*)
Процес, що має на вході підписане повідомлення, перевірковий ключ і параметри проблемної області, а на виході видає результат перевіряння підпису: підпис має силу чи ні

4.24 свідоцтво (*witness*)
Елемент даних, що забезпечує перевірювачу доказ підпису.

5 СИМВОЛИ, УГОДИ ТА УМОВНІ ПОЗНАКИ ДЛЯ РИСУНКІВ

5.1 Символи

В усіх частинах цього стандарту використовуються такі символи:

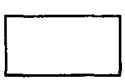
H — геш-атрибут;
$\bar{H}$ — повторно обчислений геш-атрибут;
K — рандомізатор;
M — повідомлення;
M_1, M_2 — частини підготовленого повідомлення;
R — перша частина підпису;
$\bar{R}$ — повторно обчислена перша частина підпису;
S — друга частина підпису;
T — призначення;
X — ключ підпису;
Y — перевірковий ключ;
Z — набір (один чи більше) параметрів проблемної області;
П — попередній підпис;
$\bar{\text{П}}$ — повторно обчислений попередній підпис;
Σ — підпис;
$A \bmod N$ — залишок від ділення цілого числа A на ціле число N;
$A \equiv B \pmod N$ — ціле число A конгруентне цілому числу B по модулю N, тобто $(A - B) \bmod N = 0$.

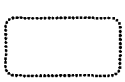
5.2 Угода щодо кодування

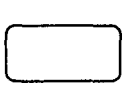
Всі цілі числа записують так, що найбільш значуща цифра (біт чи байт) знаходиться на крайній лівій позиції.

5.3 Умовні познаки для рисунків

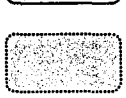
Умовні познаки для рисунків у всіх частинах цього стандарту такі:


дані;


необов'язкові процедури обробляння даних;


процедура;


основна процедура;


необов'язкова частина основної процедури;

потік даних;

необов'язковий потік даних;

два потоки даних, принаймні один з яких є обов'язковим.

6 ЗАГАЛЬНА МОДЕЛЬ

Механізм складання цифрового підпису з доповненням визначають переліком таких процесів:
— процес генерування ключа;
— процес підписування;
— процес перевіряння.

У процесі підписування підписувач обчислює свій цифровий підпис для певного повідомлення. Підпис разом з довільною частиною тексту формує доповнення, що додається до повідомлення, щоб сформувати підписане повідомлення (рисунок 1).

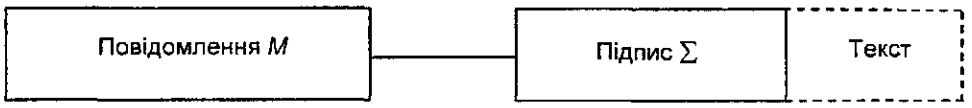


Рисунок 1 — Підписане повідомлення

Залежно від застосування є різні шляхи формування доповнення і з'єднання його з повідомленням. Головна вимога полягає в тому, щоб перевірювач зміг встановити правильний підпис до повідомлення.

Для успішного перевіряння також важливо, щоб до процесу перевіряння перевірювач зміг зв'язати правильний перевірковий ключ з підписом. Для передавання перевірювачу даних ідентифікації підписувача чи засвідченої копії його перевіркового ключа може використовуватися довільний текст. У деяких випадках є потреби в тому, щоб дані ідентифікації підписувача були частиною повідомлення *M*, так що вони стають захищеними підписом.

Механізм цифрового підписування повинен задовольняти такі вимоги:

— коли є тільки перевірковий ключ і немає ключа підпису щодо обчислювання, неможливо відтворити будь-яке повідомлення і підпис, що діє для цього повідомлення;

— підписи, виконані підписувачем, не можна використовувати як для створення будь-якого нового повідомлення, так і для відновлення ключа підпису, тому що вони мають силу підпису тільки до цього повідомлення;

— навіть підписувач щодо обчислювання не може знайти два різних повідомлення з однаковим підписом.

Примітка. Можливість обчислення залежить від специфічних вимог безпеки та оточення.

7 ЗАСОБИ ДЛЯ УВ'ЯЗУВАННЯ МЕХАНІЗМУ ПІДПИСУВАННЯ І ГЕШ-ФУНКЦІЇ

Якщо механізм цифрового підписування використовує геш-функцію, то треба ув'язати застосовані механізми підписування і геш-функції. Без такого ув'язування супротивник може претендувати на використання слабкої геш-функції (або несправжньої) і таким чином підробити підпис. Є різні засоби виконання необхідних ув'язувань. У цьому розділі наведено чотири такі засоби в порядку збільшення ризику.

Користувач механізму цифрового підпису повинен провести оцінювання ризику, розглядаючи можливі втрати і вигоди від різних альтернатив. Це оцінювання враховує втрати, пов'язані з можливістю підробити підпис.

7.1 Щоб використати специфічний механізм підписування, потрібна специфічна геш-функція. Процес перевіряння повинен використовувати тільки цю специфічну геш-функцію. В ISO/IEC 14888-3 наведено приклад такого вибору, коли механізм DSA вимагає використання SHA-1.

7.2 Є певний набір геш-функцій, і в кожному підписаному повідомленні за допомогою ідентифікатора геш-функції, включеного (як частина) в обчислення підпису, точно вказується, яка геш-функція використовувалася з передбачуваного набору геш-функцій.

Ідентифікатор геш-функції — це певне розширення геш-коду: він указує, як одержати геш-код. Процес перевіряння повинен використовувати винятково ту геш-функцію, що зазначена за допомогою ідентифікатора в підписаному повідомленні. Відповідний приклад наведено в ISO/IEC 9796-2.

7.3 У сертифікованих параметрах проблемної області точно вказується використовувана геш-функція з передбачуванного набору. У межах сертифікованої проблемної області процес перевіряння повинен використовувати винятково ту геш-функцію, що зазначена в сертифікаті. Поза цією областю є ризик використання неточних сертифікованих повноважень. Якщо можуть бути створені інші сертифікати, то можуть бути створені й інші підписи. Тоді атакований користувач може знаходитись у ситуації суперечки з сертифікованим повноваженням, що створене іншим сертифікатом.

7.4 Передбачається, що набір геш-функцій і використовувана геш-функція визначаються іншим методом, наприклад, зазначенням у повідомленні чи двосторонньою угодою. Тоді процес перевіряння повинен використовувати тільки ту геш-функцію, яка позначена цим іншим методом. Однак є ризик, що супротивник зможе підробляти підпис, використовуючи іншу геш-функцію.

8 ПРОЦЕС ГЕНЕРУВАННЯ КЛЮЧА

Процес генерування ключа в механізмі цифрового підпису складається з таких двох процедур:

— генерування параметрів проблемної області;

— генерування ключа підпису і перевіркового ключа.

Перша процедура виконується один раз, коли встановлюється проблемна область. Отриманий у результаті набір параметрів проблемної області Z необхідний у наступних процесах і функціях. Друга процедура використовується для кожного підписувача вже в межах проблемної області, і виходами для неї є ключ підпису X і перевірковий ключ Y.

Внаслідок специфіки набору параметрів проблемної області значення ключа підпису X, що буде використовуватися, з великою ймовірністю відрізняється від значень, раніше використаних.

Примітка. Може вимагатися обґрунтування параметрів проблемної області і ключів. Однак це не належить до сфери застосування цього стандарту.

9 ПРОЦЕС ПІДПИСУВАННЯ

Для процесу підписування необхідні такі елементи даних:

— параметри проблемної області Z;

— ключ підпису X;

— повідомлення M;

— ідентифікатор геш-функції (необов'язковий);

— інший текст (необов'язковий).

Для ув'язування механізму підписування і геш-функції може використовуватися ідентифікатор геш-функції (див. розділ 7).

Процес підписування з використанням механізму отримування цифрового підпису з доповненням складається з таких процедур:

— виконання попереднього підпису;

— готування повідомлення для підписання;

— обчислення свідоцтва;

— обчислення підпису.

Перша процедура необов'язкова. Механізм підписування без попереднього підпису називається детермінованим. Механізм підписування з виконанням попереднього підпису називається рандомізованим.

Свідоцтво для цифрового підпису — це елемент даних, значення якого визначають під час підписування. Правильність значення свідоцтва перевіряється в процесі перевіряння. Свідоцтво обчислюють як функцію повідомлення, або функцію попереднього підпису, або обидві разом.

Якщо свідоцтво не залежить від попереднього підпису чи попереднього підпису немає, то його називають детермінованим. Детерміноване свідоцтво не повинне передаватися перевірювачу, який також може його обчислювати, оскільки підписувач обчислює його тільки як функцію повідомлення. Процес підписування з детермінованим свідоцтвом зображений на рисунку 2.

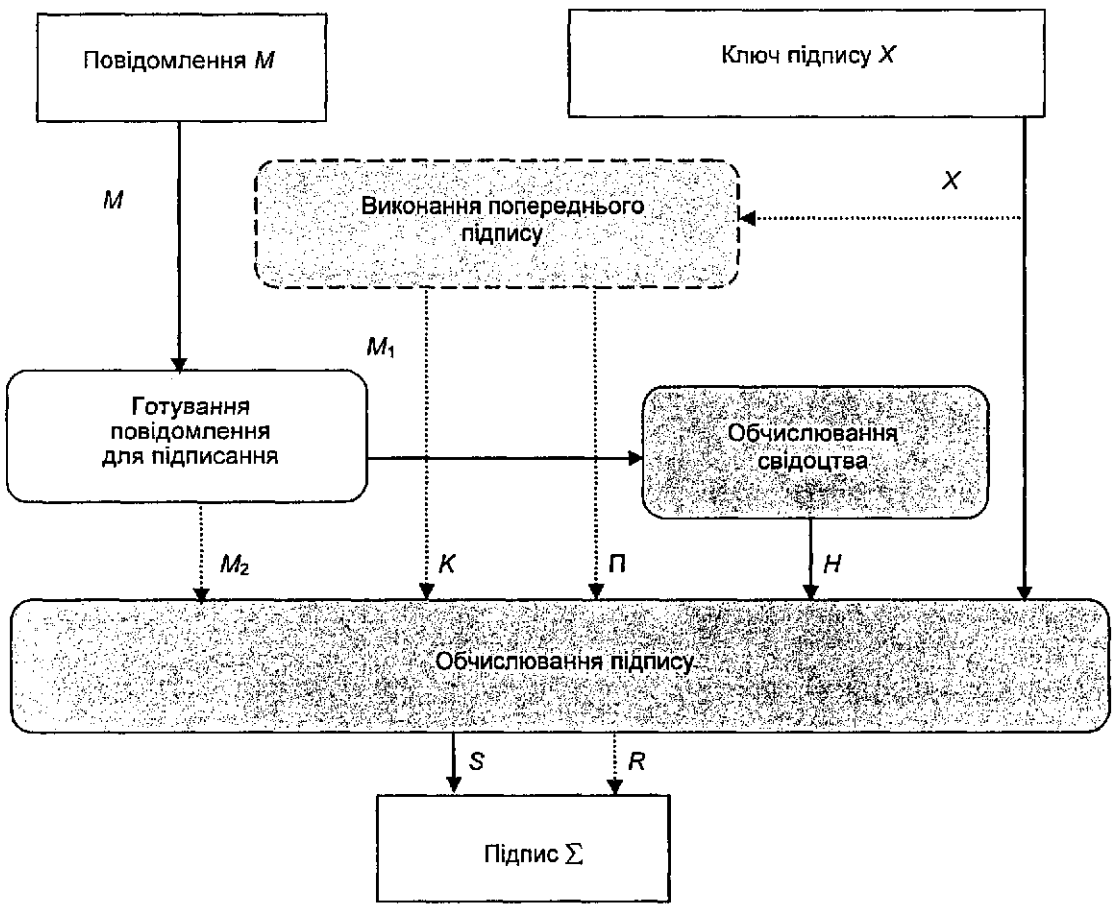


Рисунок 2 — Процес підписування з детермінованим свідоцтвом

Якщо свідоцтво залежить від попереднього підпису, воно називається рандомізованим. Значення рандомізованого свідоцтва обчислюється підписувачем, і він формує першу частину підпису. Процес підписування з рандомізованим свідоцтвом зображений на рисунку 3.

9.1 Виконання попереднього підпису

Процедура виконання попереднього підпису необхідна в рандомізованому механізмі підписування і складається з таких двох кроків:

— створення рандомізатора *K*;

— обчислення попереднього підпису П.

Результат першого кроку — рандомізатор *K*, що є секретною величиною, яку використовує тільки процес підписування. З метою збереження таємності ключа підпису для кожного повідомлення треба використовувати таке значення *K*, що з великою ймовірністю відрізняється від значень рандомізатора використовуваних раніше ключів (у межах строку служби ключа підпису). У наступному кроці попередній підпис П обчислюють через значення *K* за допомогою функції, що залежить від параметрів проблемної області *Z* та, можливо, від ключа підпису *X*. Виходами процедури виконання попереднього підпису є рандомізатор *K* та попередній підпис П.

Рисунок 3 — Процес підписування з рандомізованим свідоцтвом

Рандомізатори можна створювати, а попередні підписи обчислювати заздалегідь і секретно зберігати для подальшого використання процесом підписування. У таких випадках рандомізатор не можна обчислювати як (псевдовипадкову) функцію повідомлення.

9.2 Готування повідомлення

У процесі підписування повідомлення (чи його частини) може слугувати як вхідні дані або для обчислювання свідоцтва, або для обчислювання підпису (чи його другої частини), або і того, й іншого разом. З цією метою з повідомлення M беруть дві частини даних M_1 і M_2. Процес готування повідомлення повинен задовольняти одну з двох умов:

— повне повідомлення M повинне бути відновлюване для даних M_1 і M_2;

— щодо обчислювання неможливо знайти такі два повідомлення M та M', щоб отримані з них пари (M_1, M_2) і (M_1', M_2') були однаковими.

Характерно, що в першому випадку або $M_1 = M$, а M_2 — порожньо, або $M_2 = M$, а M_1 — порожньо, або $M_1 = M_2 = M$. В іншому випадку або M_1, або M_2, або обоє є геш-атрибутами M.

9.3 Обчислювання свідоцтва

Детерміноване свідоцтво обчислюють як геш-атрибут H повідомлення M_1 за допомогою геш-функції, стійкої до колізій (див. рис. 2). Якщо геш-функція однозначно не визначається механізмом підписування чи параметрами проблемної області, то її ідентифікатор повинен бути включений у геш-атрибут та в підписане повідомлення (див. розділ 7).

Рандомізоване свідоцтво залежить від попереднього підпису П і не обов'язково від M_1. Обчислювання рандомізованого свідоцтва як частини обчислювання підпису описане в 9.4.

9.4 Обчислювання підпису

У детермінованому механізмі входами в цю процедуру є свідоцтво H, ключ підпису X і, необов'язково, частина повідомлення M_2. У цьому випадку виходом цього кроку S і є підпис Σ (див. рис. 2).

У рандомізованому механізмі з детермінованим свідоцтвом входами в цю процедуру є рандомізатор K, ключ підпису X, детерміноване свідоцтво H та попередній підпис П. Виходом цієї процедури є повний підпис Σ, що має одну частину S чи дві частини — R і S (див. рис. 2).

У рандомізованому механізмі з рандомізованим свідоцтвом ця процедура складається з двох кроків. Спочатку обчислюється свідоцтво R, що залежить від попереднього підпису П і, необов'язково, від M_1. Якщо в обчислюванні свідоцтва використовується геш-функція, то її треба точно визначити (див. розділ 7). На другому кроці входами є рандомізатор K, ключ підпису X, рандомізоване свідоцтво R і, необов'язково, частина M_2 підготовленого повідомлення. Виходом другого кроку є S. Підпис Σ має одну частину S чи дві частини — R і S (див. рис. 3).

10 ПРОЦЕС ПЕРЕВІРЯННЯ

Для процесу перевіряння необхідні такі елементи даних:

— параметри проблемної області Z;

— перевірковий ключ Y;

— повідомлення M;

— підпис Σ;

— ідентифікатори використовуваних геш-функцій, якщо вони однозначно не визначені іншими засобами (див. розділ 7);

— інший текст (необов'язково).

Процес перевіряння механізму цифрового підписування з доповненням складається з таких процедур:

— готування повідомлення для перевіряння;

— відновлювання свідоцтва;

— обчислювання перевіркової функції;

— перевіряння свідоцтва.

Під час готування повідомлення для перевіряння може існувати потреба одержати з повідомлення M ідентифікаційні дані для ідентифікації достовірного перевіркового ключа підписувача.

Якщо свідоцтво детерміновано, то перевірювач відновлює значення свідоцтва як функцію повідомлення. Цей процес перевіряння зображений на рисунку 4.

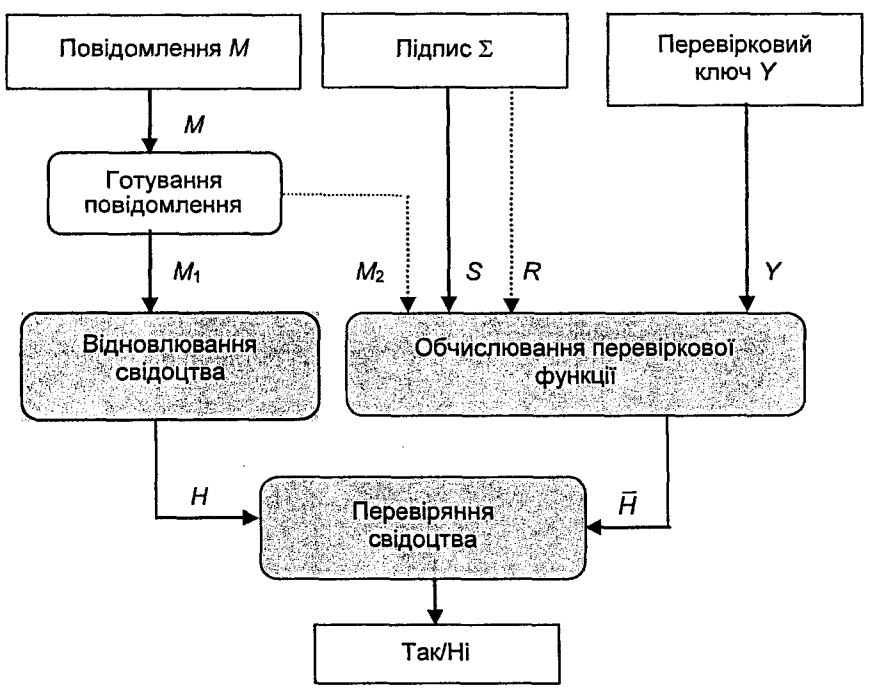


Рисунок 4 — Процес перевіряння з детермінованим свідоцтвом

Інакше (див. рис. 5) перевірювач відновлює значення свідоцтва з підпису. Перший процес перевіряння має ту перевагу, що свідоцтво можна відновлювати і повторно обчислювати паралельно.

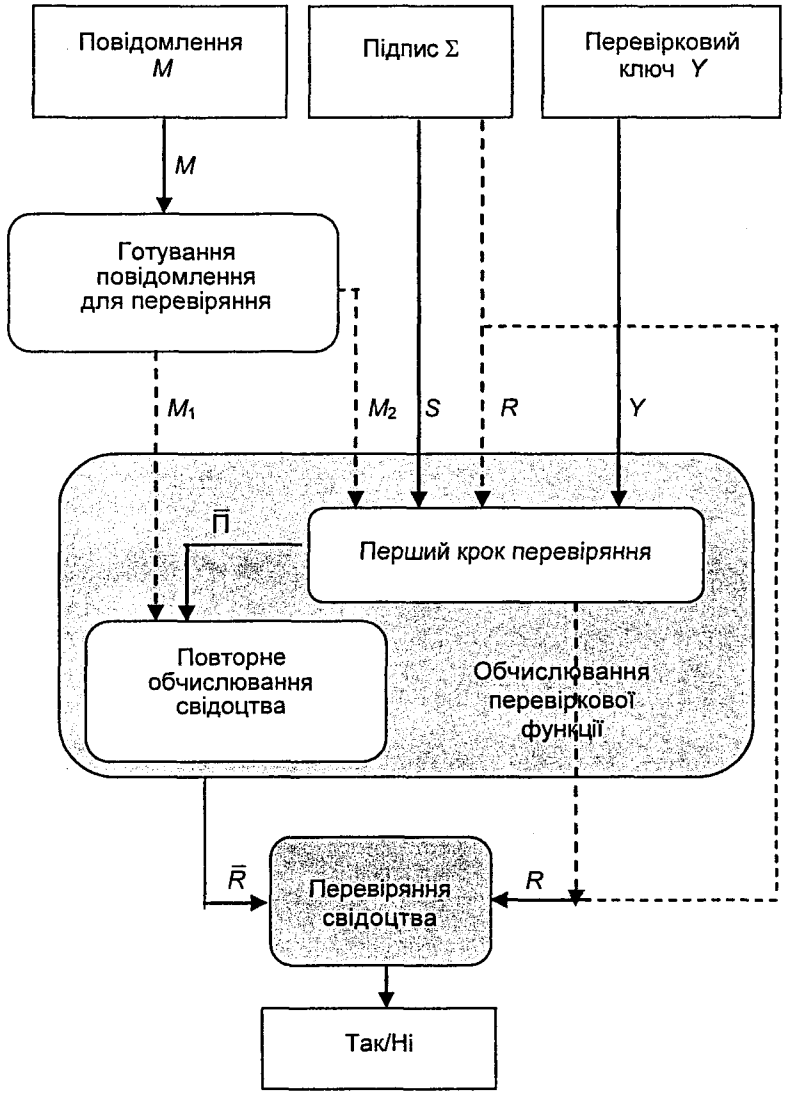


Рисунок 5 — Процес перевіряння з рандомізованим свідоцтвом

10.1 Готування повідомлення

Ця процедура повинна бути ідентична наведеній у 9.2. Входом є повідомлення *M*, а виходом — дві частини повідомлення M_1 і M_2. Якщо використовується геш-функція і якщо вона однозначно не визначена механізмом чи параметрами проблемної області, перевірювач одержує ідентифікатор геш-функції з підписаного повідомлення.

10.2 Відновлювання свідоцтва

Детерміноване свідоцтво *H* відновлюється обчислюванням його як геш-атрибута повідомлення M_1 з використанням тієї самої стійкої до колізій геш-функції, що використовувалася підписувачем у 9.3.

Якщо вона однозначно не визначена механізмом чи параметрами проблемної області, то перевірювач одержує ідентифікатор геш-функції з підписаного повідомлення.

Рандомізоване свідоцтво *R* відновлюється як перша частина підпису Σ чи як вихід перевіркової функції (див. рис. 5).

10.3 Обчислювання перевіркової функції

Перевіркова функція визначається відкритим ключем підписувача *Y*. Підпис Σ є обов'язковим входом для перевіркової функції. Якщо свідоцтво рандомізоване, частини повідомлення M_1 і M_2 з інформацією є обов'язковими входами для цього кроку (див. рис. 5). Інакше (див. рис. 4) тільки друга частина M_2, якщо вона з інформацією, є входом для перевіркової функції.

Виходом цієї процедури є повторно обчислене значення свідоцтва $\bar{H}$ або $\bar{R}$. Якщо рандомізоване свідоцтво R не є частиною підпису, то воно відновлюється перевірювачем як другий вихідний елемент цієї процедури (див. рис. 5).

10.4 Перевіряння свідоцтва

На цьому кроці порівнюються два значення свідоцтва: одне — відновлене, як пояснено в 10.2, друге — повторно обчислене (див. 10.3). Якщо ці два значення дорівнюють один одному, перевірювач одержує обґрунтування того, що підпис Σ для повідомлення M був здійснений за допомогою ключа підпису X, що відповідає перевірковому ключу Y, використаному під час перевіряння.

11 РАНДОМІЗОВАНІ МЕХАНІЗМИ З ПІДПИСАМИ, ЩО СКЛАДЕНІ З ДВОХ ЧАСТИН

У цьому розділі подані вдосконалення моделі, описаної в розділах 9 і 10. Ці вдосконалення стосуються конкретизації рандомізованих механізмів цифрового підписування, де підпис обчислюється в двох частинах.

11.1 Обчислювання підпису

Щоб обчислити підпис рандомізованим механізмом, необхідні такі елементи даних:

— параметри проблемної області Z;
— ключ підпису X;
— попередній підпис П;
— друга частина повідомлення M_2;
— детерміноване свідоцтво H чи перша частина повідомлення M_1;
— рандомізатор K;
— ідентифікатор геш-функції (необов'язковий).

В обчисленні підпису з двох частин у механізмі підписування можна виділити такі кроки:

— обчислювання першої частини підпису;
— обчислювання призначення;
— обчислювання другої частини підпису.

Для механізму з детермінованим свідоцтвом ці кроки зображені на рисунку 6, що є розширенням блоку «обчислювання підпису» рисунка 2 для спеціального випадку рандомізованих механізмів.

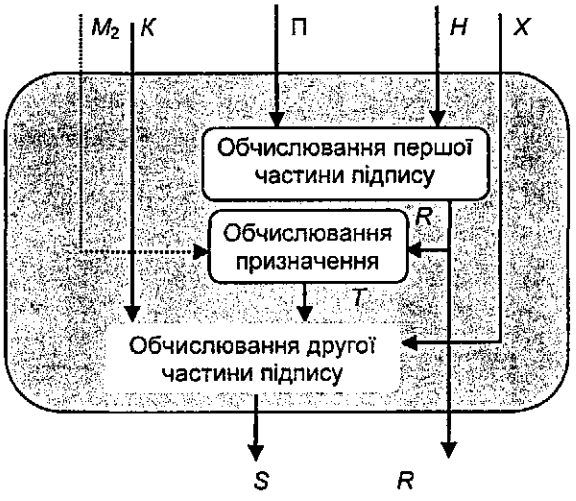


Рисунок 6 — Обчислювання підпису рандомізованим механізмом з детермінованим свідоцтвом

Якщо свідоцтво рандомізоване, воно є першою частиною підпису. Кроки, необхідні для обчислювання підпису, зображені на рисунку 7, що є розширенням блоку «обчислювання підпису» (див. рис. 3).

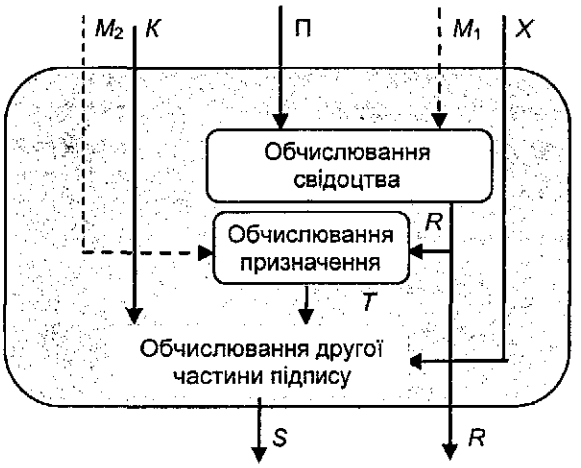


Рисунок 7 — Обчислювання підпису з рандомізованим свідоцтвом як частини підпису

Потрібно, щоб для всіх значень попереднього підпису щодо обчислювання було неможливо знайти два повідомлення з однаковим свідоцтвом і призначенням. У більшості рандомізованих механізмів цифрового підписування або $M_1 = M$, а M_2 — порожньо, або M_1 — порожньо, а $M_2 = M$.

У першому випадку свідоцтво H чи R обчислюється за допомогою геш-функції, стійкої до колізій. У другому випадку, де M_1 — порожньо, свідоцтво залежить тільки від попереднього підпису, а призначення T обчислюється за допомогою геш-функції, стійкої до колізій. Якщо геш-функція однозначно не визначена механізмом підписування чи параметрами проблемної області, до призначення треба включити ідентифікатор геш-функції.

11.1.1 ***Обчислювання першої частини підпису***

Якщо свідоцтво рандомізоване, воно є першою частиною підпису. Його обчислюють так, як описано в 9.4.

Якщо свідоцтво детерміноване, то входами для цього кроку є свідоцтво H і попередній підпис П. Виходом буде R — перша частина підпису. Цей процес обчислювання повинен бути зворотній в такому розумінні: за заданими R і П перевірювач повинен обчислити H.

11.1.2 ***Обчислювання призначення***

Входом для цього кроку є R — перша частина підпису, а також, можливо, частина повідомлення M_2, а виходом буде призначення T.

11.1.3 ***Обчислювання другої частини підпису***

Функція підпису визначається ключем підпису X, на вході їй потрібні рандомізатор K і призначення T, а на виході вона видає значення другої частини підпису S.

У деяких механізмах підписування функція підпису подається як рівняння, визначене набором параметрів з X, K і T та S як невідомого.

11.2 Обчислювання перевіркової функції

Для обчислювання перевіркової функції необхідні такі елементи даних:

— параметри проблемної області Z;
— перевірковий ключ Y;
— підпис $\Sigma = (R, S)$;
— друга частина повідомлення M_2 (необов'язковий);
— ідентифікатор геш-функції (необов'язковий).

Процес перевіряння рандомізованого механізму підписування складається з таких кроків:

— відновлення призначення;
— повторного обчислювання попереднього підпису;
— повторного обчислювання свідоцтва.

Для рандомізованих механізмів з детермінованим свідоцтвом ці кроки зображені на рисунку 8, що є розширенням відповідного блоку (див. рис. 4) для спеціального випадку рандомізованих механізмів. Якщо свідоцтво рандомізоване, воно обчислюється повторно, як зображено на рисунку 9, що є вдосконаленою версією відповідного блоку (див. рис. 5).

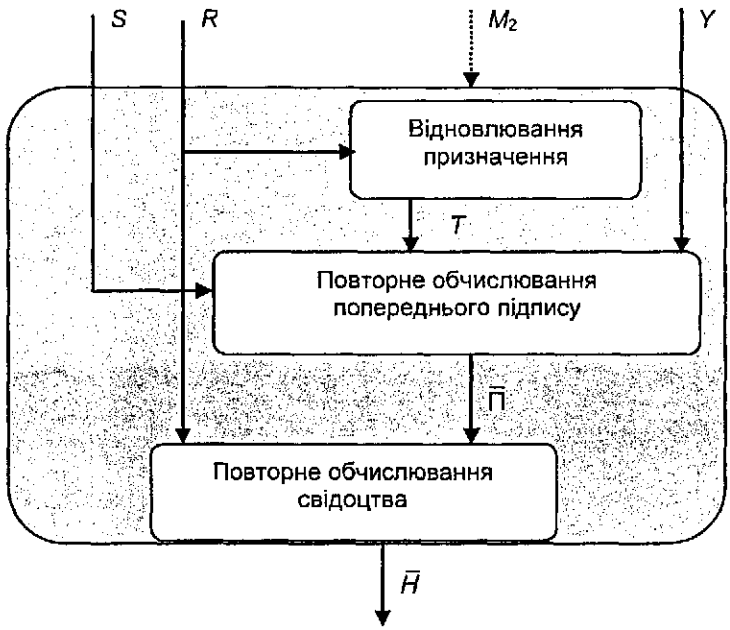


Рисунок 8 — Обчислювання перевіркової функції в рандомізованому механізмі з детермінованим свідоцтвом

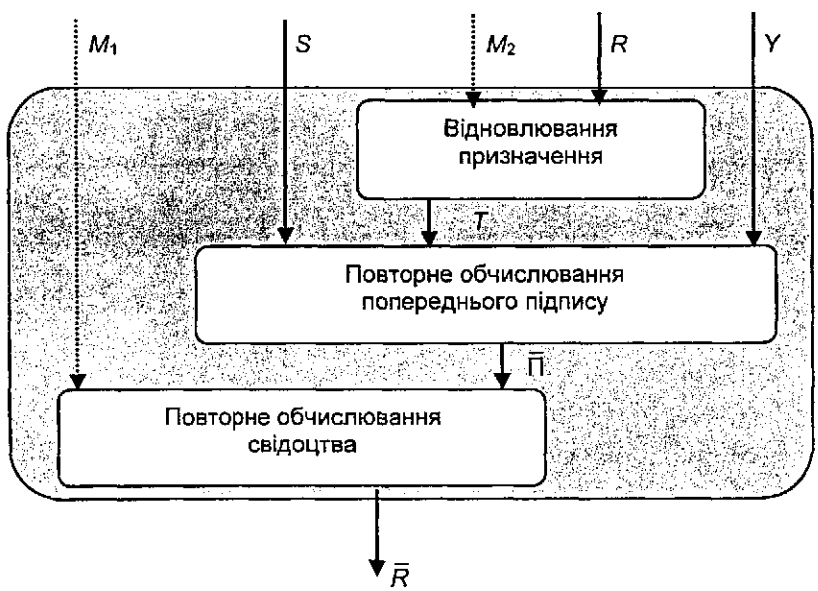


Рисунок 9 — Обчислювання перевіркової функції в рандомізованому свідоцтві як частини підпису

11.2.1 ***Відновлення призначення***

Цей крок ідентичний 11.1.2. Виходом його є призначення *T*.

11.2.2 ***Повторне обчислювання попереднього підпису***

Цей крок визначається перевірковим ключем *Y*. Іншими входами в нього є друга частина підпису *S* і призначення *T* з 11.2.1. Виходом буде повторно обчислене значення попереднього підпису $\bar{П}$.

11.2.3 ***Відновлювання призначення***

Цей крок ідентичний 11.1.2. Виходом його є призначення T.

11.2.4 ***Повторне обчислювання попереднього підпису***

Цей крок визначається перевірковим ключем Y. Іншими входами в нього є друга частина підпису S і призначення T з 11.2.1. Виходом буде повторно обчислене значення попереднього підпису $\bar{\Pi}$.

11.2.5 ***Повторне обчислювання свідоцтва***

Якщо свідоцтво детерміноване, то відповідно до умови кроку 11.1.1 перевірювач згодний повторно обчислити значення свідоцтва $\bar{H}$ з першої частини підпису R, використовуючи повторно обчислене значення попереднього підпису $\bar{\Pi}$ (див. рис. 8).

Якщо свідоцтво рандомізоване, то перевірювач використовує ту саму обчислювальну процедуру, що й підписувач в 9.3, щоб визначити повторно обчислене значення свідоцтва $\bar{R}$ залежно від повторно обчисленого попереднього підпису $\bar{\Pi}$ і, необов'язково, від першої частини повідомлення (див. рис. 9).

УКНД 35.040

Ключові слова: безпека інформації, геш-атрибут, геш-функція, детерміноване свідоцтво, захист, перевіркова функція, перевірковий ключ, повідомлення, рандомізатор.

Редактор **Є. Козир**
Технічний редактор **О. Марченко**
Коректор **О. Ніколаєнко**
Верстальник **С. Павленко**

Підписано до друку 06.12.2006. Формат 60 × 84 1/8.
Ум. друк. арк. 1,86. Зам. 4091 Ціна договірна.

Відділ редагування нормативних документів ДП «УкрНДНЦ»
03115, Київ, вул. Святошинська, 2