ПРОТОКОЛ ГРУПОВОГО ЦИФРОВОГО ПІДПИСУ НА ОСНОВІ УКРАЇНСЬКОГО СТАНДАРТУ ДСТУ 4145-2002

Козіна Г. Л.[1], к.ф.-м.н., доцент; Савченко Д. К.[1], аспірант
[1] ЗНТУ, м. Запоріжжя, Україна

В даній роботі авторами пропонується груповий підпис, що відповідає таким властивостям:

а) тільки члени групи можуть підписувати повідомлення;
б) одержувач може перевірити, що підпис дійсно належить групі підписуючих, але не може знати особу, що його створила;
в) за необхідності, підпис може бути "відкритий", так що виявляється особа, яка підписала повідомлення;
г) особисті секретні ключі представників групи і Лідера нікому не розголошуються;
д) Лідер за значенням підпису і відповідного йому документу може визначити особу, що сформувала даний конкретний підпис;
е) Лідер формує групу підписантів та документ;
ж) частини документу, які потрібно підписати членам групи розподіляє Лідер;
з) використання додаткового параметру U, який містить інформацію про членів групи та частини документу, які вони підписують.

Груповий підпис в запропонованому протоколі включає в себе підписи представників групи, які затверджуються підписом керівника (Лідера).

Формування протоколу групового підпису з такими якостями необхідно для забезпечення схожості процедури підписання електронних документів з паперовими документами, які необхідно підготувати, підписати та затвердити.

Схема побудови пропонованого групового підпису включає як свою внутрішню частину механізм формування композиційного підпису. Даний механізм використовує обчислення композиційного параметра підпису, за яким всі особи, що входять до складу групи, обчислюють свої частини підпису відповідних документів.

Загальносистемні параметри обираються згідно з ДСТУ 4145-2002: еліптична крива $y^2 + xy = x^3 + Ax^2 + B$, базова точка еліптичної кривої P простого порядку n, δ – допоміжне просте багаторозрядне двійкове число (введення допоміжного числа δ дозволяє скоротити першу частину цифрового підпису).

Кожний потенційний представник групи має асиметричну пару ключів: особистий $d_i s$, $1 < d_i < n$, та відкритий $Q_i = -d_i P$. Лідер групи також має асиметричну пару ключів: особистий d_L, $1 < d_L < n$, та відкритий $Q_L = -d_L P$

Формування цифрового підпису проходить наступним чином: нехай

Лідер сформував групу із t представників підписати електронний документ $M = \sum\{M_1, M_2, ..., M_t\}$, причому кожен користувач i, $i = 1,2,...,t$, має підписати свій електронний документ M_i з геш-образом $H(M_i)$, якому відповідає десяткове число h_i.

Кожен представник групи надає Лідеру свій відкритий ключ Q_i, а Лідер надає йому на підписання відповідний документ M_i. Лідер групи обчислює геш-образи $H(M_i)$ документів і формує відповідні десяткові числа h_i із $|n|-1$ молодших розрядів геш-образів $H(M_i)$. Далі Лідер обчислює перший елемент групового підпису U: $U = \sum_{i=1}^{t} h_i \cdot Q_i$.

Кожний представник групи обирає одноразовий випадковий секретний ключ k_i , $1 < k_i < n$, обчислює точку еліптичної кривий $R_i = k_i P$ та надає її Лідеру для подальшого використання.

Лідер також обирає одноразовий випадковий секретний ключ k_L, $1 < k_L < n$, обчислює точку $R_L = k_L P$ та суму всіх точок R_i, $i = 1,2,...,t$, і R_L: $R = \sum_{i=1}^{t} R_i + R_L = (xR, yR)$, після чого формується другий елемент групового підпису – число r.

Молодші $|n|-1$ розряди елемента поля xR формують десяткове число u. Число r обчислюється за формулою $r = u \bmod \delta$ і не повинно бути 0. При $r = 0$ обираються нові випадкові секретні ключі k_i.

Потім кожний представник групи за допомогою свого секретного ключа d_i та значення k_i обчислює свою частину підпису $s_i = k_i + r \cdot d_i \cdot h_i \bmod n$ та надає її Лідеру.

Лідер перевіряє справжність кожного підпису s_i за допомогою відповідного відкритого ключа підписанта Q_i. Якщо виконується співвідношення $s_i P + r \cdot h_i \cdot Q_i = R_i$ підпис признається справжнім.

Далі Лідер обчислює геш-образ $H(M)$ документа M, формує відповідне десяткове число h із $|n|-1$ молодших розрядів геш-образу $H(M)$ і також за допомогою секретного ключа d_L та значення k_L обчислює свою частину підпису $s_L = k_L + r \cdot d_L \cdot h \bmod n$, після чого генерується число s – третій елемент підпису: $s = (s_L + \sum_{i=1}^{t} s_i) \bmod n$. Число s не може бути рівним 0. При $s = 0$ процедура підпису повторюється.

Груповим підписом є трійка $\langle U, r, s \rangle$.

Перевірка групового підпису $\langle U, r, s \rangle$ під електронним документом M

здійснюється за допомогою додаткової точки еліптичної кривої $Q = U + h \cdot Q_L$, яка залежить від геш-образу h документа M та відкритого ключа Лідера групи Q_L.

Обчислюються точка RR: $RR = sP + r \cdot Q = (xRR, yRR)$. Молодші $|n|-1$ розряди елемента поля xRR формують десяткове число $\tilde{u}$. Число $\tilde{r}$ обчислюється за формулою $\tilde{r} = \tilde{u} \mod \delta$.

Якщо $\tilde{r} = r$, груповий цифровий підпис електронного документу M признається справжнім.

Запропонований протокол групового підпису ґрунтується на українському державному стандарті підпису ДСТУ 4145-2002, тому його можна вважати захищеним від підробки. Порівняно з розміром підпису згідно зі стандартом, розмір групового підпису збільшується за рахунок використання додаткового параметру U, який містить інформацію про членів групи та відповідні їм частини документу M. Оскільки U є точкою еліптичної кривої над полем $GF(2^m)$, розмір підпису збільшується на $2 \times m$ біт. Але загальний розмір підпису частково компенсується за рахунок зменшення другої частини підпису r, яка залежить від обраного значення δ – допоміжного простого багаторозрядного числа. Тобто спостерігається незначне збільшення розміру групового підпису порівняно з розміром підпису, що засновано на стандарті ДСТУ 4145-2002.

Анотація

Розглянуто протокол групового електронного цифрового підпису в групі точок еліптичної кривої на основі українського стандарту ДСТУ 4145-2002. Розроблено алгоритм формування підпису в групі з різними повноваженнями підписантів за принципом композиційного підпису.

Ключові слова: електронно-цифровий підпис, протокол групового підпису, композиційний підпис, ДСТУ 4145-2002

Аннотация

Рассмотрен протокол групповой электронной цифровой подписи в группе точек эллиптической кривой на основе украинского стандарта ДСТУ 4145-2002. Разработан алгоритм формирования подписи в группе с разными полномочиями подписывающих по принципу композиционной подписи.

Ключевые слова: электронно-цифровая подпись, протокол групповой подписи, композиционная подпись, ДСТУ 4145-2002.

Abstract

The digital group signature protocol based on Ukrainian digital signature standard DSTU 4145-2002 is considered. The algorithm for signature generation in the group with different authority of the signatories on the basis of the composite signatures has been developed.

Keywords: digital signature, group signature protocol, compositional signature, DSTU 4145-2002.