УДК 681.3: :002.651.028(083.73)

Мелащенко А. О., Перевозчикова О. Л., Скарлат О. С., Криворучко К. С.

КОМПЛЕКТИ ПІДПИСІВ ДЛЯ ІНТЕРОПЕРАБЕЛЬНОСТІ НАЦІОНАЛЬНОЇ СИСТЕМИ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ

Проаналізовано можливості зворотної підтримки нині чинних і застосовних криптографічних алгоритмів і геш-функцій в модифікованій інтероперабельній, з можливістю кроссертифікації Національній системі електронного цифрового підпису України. Також наведено відповідність перелічених в ДСТУ ETSI TS 102 176-1 стандартів з гармонізованими ДСТУ.

Вступ

Проблеми інтероперабельності Національної системи електронних цифрових підписів (НСЕЦП) України зумовили потребу кардинальної переробки її організаційної й технологічної бази. Для досягнення внутрішньої інтероперабельності та можливості кроссертифікації України з ЄС і цілим світом потрібен Технічний регламент, підтриманий ДСТУ, гармонізовано з міжнародними стандартами.

Згідно з [1] базовою складовою кваліфікованої інфраструктури відкритих ключів (QPKI) є комплекти підпису. Внаслідок хуторянської позиції щодо НСЕЦП в Україні впроваджено локальні алгоритми підписування й геш-функції, які не дають змоги кроссертифікуватися з жодною країною світу. Нині не регламентовано використання й опис комплектів підпису, а впровадження [2] сприятиме розв'язанню цієї проблеми. Проте в [2] існують посилання на першоджерела складових комплектів підпису, які треба відобразити у чинних ДСТУ.

Далі проаналізовано можливості зворотної підтримки нині чинних і застосовних криптоалгоритмів та геш-функцій в модифікованій інтероперабельній з можливістю кроссертифікації НСЕЦП України. Також наведено відповідність зазначених в [2] стандартів з гармонізованими ДСТУ.

Комплекти підпису

Щоб виконати вимоги безпеки й дати змогу підписувати повідомлення довільної довжини, у комплект підпису входить геш-функція. Важлива проблема – зв'язок геш-функції зі схемою підписування, без цього найслабша доступна геш-функція може встановити загальний рівень безпеки.

Через можливі взаємодії, здатні вплинути на захист ІТ, алгоритми й параметри для надійних засобів ЕЦП необхідно використовувати тільки у визначених комбінаціях, іменованих комплектами підпису. Комплект підпису складено з трьох компонентів: геш-функція, метод доповнення, алгоритм підписування з набором параметрів.

Якщо змінено кожний з компонентів комплекту, то комплект змінюють відповідно. Перелік чинних в Україні та рекомендованих ETSI комплектів підпису, наведено у табл. 1.

Таблиця 1. **Рекомендовані ETSI комплекти підписів**

Ім'я комплекту підпису	Ім'я геш-функції	Ім'я методу доповнення	Ім'я алгоритму підписання
sha 1-with-rsa	sha1	Вибирається з [8]	rsa
sha 1-with-dsa	sha1	не потребує доповнення	dsa
ripemd 160-with-rsa	ripemd160	Вибирається з [8]	rsa
ripemd 160-with-dsa	ripemd160	не потребує доповнення	dsa
sha 224-with-rsa	sha224	Вибирається з [8]	rsa
sha 256-with-rsa	sha256	Вибирається з [8]	rsa
rsa-pss з mgflSHA-1Identifier	mgf1 SHA-1		rsa
rsa-pss з mgf1 SHA-224Identifier	mgf1 SHA-224		rsa
rsa-pss з mgf1 SHA-256Identifier	mgf1 SHA-256		rsa
sha 1-with-ecdsa	sha1	не потребує доповнення	ecdsa-Fp або ecdsa-F2m
sha 1-with-ecgdsa	sha1	не потребує доповнення	ecgdsa-Fp або ecgdsa-F2m
sha 224-with-ecdsa	sha224	не потребує доповнення	ecdsa-Fp або ecdsa-F2m
sha 256-with-ecdsa	sha256	не потребує доповнення	ecdsa-Fp або ecdsa-F2m
sha 384-with-ecdsa	sha384	не потребує доповнення	ecdsa-Fp або ecdsa-F2m
sha 512-with-ecdsa	sha512	не потребує доповнення	ecdsa-Fp або ecdsa-F2m
ecdsa-with-RIPEMD160	ripemd160	не потребує доповнення	ecdsa-Fp або ecdsa-F2m

Тут:

1) sha1 (Secure Hash Algorithm 1) – алгоритм гешування. Для вхідного повідомлення довільної довжини (максимум $2^{64} - 1$ біт) алгоритм генерує 160-бітне значення гешу.
2) ripemd160 – алгоритм гешування з довжиною результуючого геш-значення в 160 біт.
3) sha224, sha256 – алгоритми гешування. Для вхідного повідомлення довільної довжини (максимум $2^{64} - 1$ біт) відповідно генерується 224- і 256-бітне геш-значення.
4) sha384, sha512 – алгоритми гешування. Для вхідного повідомлення довільної довжини (максимум $2^{128} - 1$ біт) відповідно генерується 384- і 512-бітне геш-значення.
5) dsa (Digital Signature Algorithm) – криптоалгоритм для створення ЕЦП.
6) rsa (Rivest, Shamir і Adleman) – криптоалгоритм для створення ЕЦП і шифрування.
7) ecdsa (Elliptic Curve Digital Signature Algorithm), ecgdsa (Elliptic Curve German Digital Signature Algorithm) – криптоалгоритми для ЕЦП, визначені над полями точок еліптичної кривої.

З комплектом підпису асоційовано рекомендовані терміни стійкості комплекту в цілому.

Комплекти підпису будують за модульним принципом, що сприяє розвитку конкуренції серед розробників компонентів. За потреби легко замінити будь-яку складову, а реалізація загального механізму комплектів підписів допомагає створювати їх з багатьох готових (сертифікованих) компонентів.

Інтероперабельність криптоалгоритмів

Насамперед НСЕЦП неінтероперабельна через відсутність профілів на два базових криптоалгоритми [3, 4] та нерозробленість стандартів на формати базових компонентів. Для максимізації інтероперабельності для застосування ЕЦП у конкретних середовищах необхідно ідентифікувати єдиний набір опцій, застосовних у цьому середовищі. Такий набір називають профілем і зазвичай закріплюють об'єктним ідентифікатором (OID). В Україні немає профілів на застосовні криптоалгоритми та геш-функції, більше того, не створено узгоджені формати та протоколи для інтероперабельного впровадження криптомодулів в НСЕЦП.

Іншою проблемою є формат сертифіката, введений згідно з Наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ та Держдепартаменту з питань зв'язку та інформатизації Мінтрансу [5], що жорстко обмежив використання криптоалгоритмів [3, 4]. Згідно зі статтею 11 Закону України «Про стандартизацію» в Україні чинні тільки національні стандарти (ДСТУ). Згідно з чинними з 2005 р. ДСТУ [7–9] вже чотири роки можна впроваджувати міжнародні комплектів підписів, але згаданий Наказ [5] унеможливлює їх поширення. Виходом може стати прийняття нового наказу про формат сертифіката, який ґрунтується на [10], до прийняття Технічного регламенту НСЕЦП. Зазначимо, що реалізувати чинний наказ [5] вкрай важко через відсутність у ньому повного лістингу ASN.1-нотації формату сертифіката. Сумнівна правильність наведених у наказі [5] технічних специфікацій, оскільки кожна з частин ISO/IEC 8824-8825 має по кілька коригувань, нехтувати якими заборонено. У розроблений нами текст проектів ДСТУ, гармонізованих з ISO/IEC 8824-8825, включено усі коригування, від чого обсяг зріс на 80%. Невідомо, яким же чином контролюючий орган оцінює та видає експертні висновки, що «…формати відкритих ключів та списки відкликаних сертифікатів відповідають вимогам Технічних специфікацій форматів подання базових об'єктів», затверджених наказом [5]?

Для досягнення внутрішньої/зовнішньої інтероперабельності доцільно використовувати сертифіковані й тому інтероперабельні міжнародні бібліотеки. Так, бібліотека OpenSSL з відкритим кодом (http://openssl.org) застосовна у UNIX-подібних операційних середовищах і реалізує міжнародні геш-функції SHA-1, RIPEMD-128 та -160, SHA-224, -256, -384 та SHA-512, WHIRPOOL і криптоалгоритми RSA, DSA, ECDSA-Fp, ECDSA-F2m, ECGDSA-Fp, ECGDSA-F2m.

Поняття комплектів підписів вводить ДСТУ [2], створює нормативну базу для побудови модульних і стійких комплектів підписів. Але це ДСТУ посилається не тільки на міжнародні стандарти, а й на національні, для його впровадження треба довести наявність всіх складових комплектів підписів. У [2] визначено списки геш-функцій і схеми підписування у формі комплектів підписів. Далі проаналізовано перетин санкціонованих ЄС комплектів підписів, зазначених в [2], з гармонізованими ДСТУ [8, 9]. З огляду на потребу в перегляді [11], розглянуто перетин алгоритмів старої редакції [8], чинної в Україні, і нової [11], зазначено санкціоновані в Україні комплекти підписів й їхній склад, надано рекомендації щодо розробки стандартів для повної підтримки [2].

Аналіз алгоритмів підписування згідно з ETSI TS 102 176 і ISO/IEC 14888:2002. Стандарт ДСТУ ETSI TS 102 176-1 (V2.0.0) описує схеми підпису, до яких входять алгоритми підписування й методи генерації пари ключів. Стандарт не описує всі алгоритми, які підходять для розширених електронних підписів, а обмежує цей список раціональним набором для досягнен-

ня інтероперабельності. Інтероперабельність із безпекою є основним завданням функціонування програмно-технічних комплексів, які забезпечують послуги НСЕЦП. Основний критерій для включення алгоритму в стандарт – факт того, що алгоритм є «безпечний, поширений і розгорнутий на практиці». Список рекомендованих цим стандартом алгоритмів підписування включає RSA, DSA, ECDSA-Fp, ECDSA-F2m, ECGDSA-Fp, ECGDSA-F2m.

Чинний ДСТУ ISO/IEC 14888-3:2002, гармонізований із ISO/IEC 14888-3:1998, містить опис алгоритмів підписування на основі дискретних логарифмів: алгоритми підписування, які базуються на еліптичних кривих: DSA на еліптичних кривих, ECDSA на еліптичних кривих Fp і F2m – адитивна група та алгоритми DSA, мультиплікативна група Pointcheval/Vaudenay. В [2] зазначено, що алгоритм ECGDSA – це варіант алгоритму ECDSA зі зміненим рівнянням створення підпису й методом верифікації. ECGDSA – зручний для проектування й роботи з безпечним засобом створення підписів.

Наявні в ДСТУ та санкціоновані ЄС набори алгоритмів підписування наведено в табл. 2. Зазначимо, що стара редакція [8] не містить всіх потрібних алгоритмів підписування.

Таблиця 2. **Перетин наборів алгоритмів підписування ДСТУ ISO/IEC 14888:2002 та ДСТУ ETSI TS 102 176-1 (V2.0.0)**

Крипто-алгоритм	ДСТУ ISO/IEC 14888:2002	ISO/IEC 14888:2008	ДСТУ ETSI TS 102 176
RSA	+	+	+
DSA	+	+	+
ECDSA- F_p	+	+	+
ECDSA- F_{2^m}	+	+	+
ECGDSA- F_p	–	+	+
ECGDSA- F_{2^m}	–	+	+
Pointcheval/ Vaudenay	+	+	–
ESIGN	+	+	–
GQ1	–	+	–
GQ2	–	+	–
GPS1	–	+	–
GPS2	–	+	–

Аналіз алгоритмів підписування згідно з ДСТУ ETSI TS 102 176 та ISO/IEC 14888:2008. Нова редакція [8] містить розширений список алгоритмів підписування, покриваючи всі рекомендовані алгоритми, а також включає нові.

Аналіз геш-функцій ДСТУ ETSI TS 102 176 та ДСТУ ISO/IEC 10118. В ДСТУ ETSI TS 102 176-1 (V2.0.0) описано геш-функції в контексті їхнього використання й визначення основних трьох властивостей: спротив передбаченню, 2-й спротив передбаченню й спротив колізіям. Відповідно до наданого опису, визначено ряд рекомендованих геш-функцій: SHA-1, RIPEMD-160, SHA-224, SHA-256, WHIRPOOL, SHA-384, SHA-512. Чинний ДСТУ ISO/IEC 10118-3:2005 описує основну модель геш-функцій, їхні параметри, методи заповнення, раундові функції й узгодження порядку проходження байтів, за допомогою яких побудовано спеціалізовані геш-функції. У цьому стандарті геш-функцій ґрунтуються на повторному використанні раундової функції. Визначено сім різних раундових функцій, які породжують різні спеціалізовані геш-функції. Детально описано сім геш-функцій RIPEMD-160, RIPEMD-128, SHA-1, SHA-256, SHA-512, SHA-384, WHIRPOOL.

Опираючись на зазначені геш-функції, у стандарті ДСТУ ETSI TS 102 176-1 (V2.0.0) розглянуто найважливіші з них для досягнення інтероперабельності. Для детального опису геш-функції, зокрема параметрів, функцій, констант, початкових значень, методів заповнення й з'ясування раундової функції, у ДСТУ ETSI TS 102 176-1 (V2.0.0) є посилання на FIPS Publication 180-2 і відповідно на ДСТУ ISO/IEC 10118-3:2005.

Перетин набору геш-функцій наведено в табл. 3. Найефективнішою геш-функцією зараз вважають WHIRPOOL, тільки її рекомендовано в [2] для обчислення значення гешу токена часового штемпеля. Хоча геш-функції SHA-224 і SHA-384 рекомендовано у [2], їх бажано не застосовувати із причин інтероперабельності: вони не мають переваг безпеки й обчислень. Згідно з ДСТУ[2] геш-функції SHA-1 і RIPEMD-160 все ще безпечні, але рекомендовано перейти на комплекти підпису з розміром результату, більшим за 160 бітів. Для довготермінових підписів рекомендовано WHIRPOOL і SHA-512, для короткотермінових – SHA-256.

Таблиця 3. **Перетин набору геш-алгоритмів ДСТУ ISO/IEC 10118 та ДСТУ ETSI TS 102 176-1 (V2.0.0)**

Геш-функція	ДСТУ ISO/IEC 10118	ДСТУ ETSI TS 102 176
SHA-1	+	+
RIPEMD-128	+	–
RIPEMD-160	+	+
SHA-224	–	+
SHA-256	+	+
SHA-384	–	+
SHA-512	+	+
WHIRPOOL	+	+

Аналіз методів рандомізації, рекомендованих ДСТУ ETSI TS 102 176-1. У [2] визначено два генератори випадкових чисел: trueran і pseuran, які висувають вимоги до недетермінованих NRNG і детермінованих DRNG генераторів

випадкових чисел. Методи trueran рекомендовано для генерації часто застосовних ключів. Для рідко застосовних ключів ці вимоги послаблено для DSA, ECDSA і ECGDSA. Класифікацію генераторів випадкових чисел згідно з [2] наведено на рис. 1.

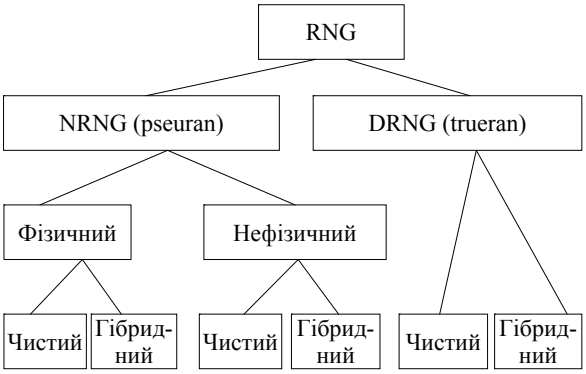

Рис. 1. Класифікація генераторів випадкових чисел згідно з ДСТУ ETSI TS 102 176-1

В Україні санкціоновано генератор випадкових послідовностей, визначений у [3], цей генератор є недетермінований NRNG із фізичним джерелом ентропії.

Впровадження [2] розширить перелік санкціонованих генераторів випадкових чисел.

Аналіз методів доповнення, рекомендованих ДСТУ ETSI TS 102 176-1 (V2.0.0). Методи доповнення залежать від обраного алгоритму підписування. Зокрема алгоритми DSA, ECDSA, ECGDSA не потребують доповнення. Для схеми RSA потрібно нетривіальне доповнення методом кодування повідомлення в цілочислове подання, що буде входом до примітиву підпису. Таке кодування може бути детермінованим, коли фіксовану послідовність доповнюють фіксованим текстовим полем до значення гешу, обчисленого з повідомлення, або рандомізованим, коли фіксовану послідовність доповнюють випадково згенерованим значенням «солі», причому її довжина перевищує параметри обраного генератора випадкових чисел. У табл. 4 зазначено методи доповнення [2]. Зауважимо, що поки не виявлено атаки на метод доповнення emsa-pkcs1-v1.5, але його використовувати не рекомендовано через моральне старіння. Метод emsa-pss не набув поширення, проте засвідчив стійкість і придатний для довготермінового використання.

Відповідно до стандарту [8] доповнення будують із підпису й додаткового текстового поля, що може включати сертифікат, який криптографічно пов'язує відкритий ключ із даними ідентифікації підписувача. У [8] описано останні три методи доповнення. Для впровадження перших трьох потрібен Технічний регламент з НСЕЦП.

Таблиця 4. **Методи доповнення згідно з ДСТУ [2]**

Індекс генератора ключів	Ідентифікатор методу доповнення	Метод генерації випадкових чисел
4.01	emsa-pkcs1-v1.5	–
4.02	emsa-pkcs1-v2.1	–
4.03	emsa-pss	trueran/pseuran
4.04	iso9796ds2	trueran/pseuran
4.05	iso 9796-din-rn	trueran/pseuran
4.06	iso9796ds3	–

Результати аналізу показали досить повну готовність сукупності національних стандартів України для впровадження міжнародних комплектів підпису, для цього треба виконати три кроки:

1. Терміново ввести новий формат сертифіката відкритого ключа з терміном дії документа «до прийняття Технічного регламенту з НСЕЦП».
2. Негайно переглянути ДСТУ ISO/IEC 14888:2002 для гармонізації із ISO/IEC 14888:2008.
3. Розробити та впровадити Технічний регламент НСЕЦП.

Зворотна сумісність нової й старої версії НСЕЦП. Для впровадження міжнародних стандартів необхідно забезпечити зворотну сумісність ДСТУ чинних, гармонізованих з міжнародними стандартами. Оскільки ДСТУ й ГОСТ побудовано на відомих принципах, необхідно проаналізувати їхню можливу реалізацію в міжнародних стандартах. Отже, можна «згорнути» набір стандартів, застосовних в Україні, до міжнародних стандартів і алгоритмів. Для цього треба зіставити [3–4] на відповідність останній редакції [11] і чинній в Україні старій редакції [8].

Аналіз алгоритмів підпису відповідно до ГОСТ 34.310:1995 і ДСТУ ISO/IEC 14888-1:2002. Чинні ДСТУ [4] і [8] ґрунтуються на алгоритмах і механізмах, заснованих на методах асиметричної криптографії. Існують три основних етапи для кожного асиметричного механізму цифрового підписування, а саме процес:

– генерування пари ключів, складеної з особистого ключа й відповідного відкритого ключа;
– який використовує особистий ключ й називається процесом підписування;
– який використовує відкритий ключ і називається процесом верифікації підпису.

Алгоритм підписування [4] відповідає алгоритму підписування з використанням рандомізованного механізму з детермінованим доказом з [8]. Аналіз відповідності кроків і перетин алгоритмів процесу підписування [4] і [8] наведено в табл. 5.

Таблиця 5. **Аналіз відповідності перетину кроків алгоритмів підписування**

Кроки підписування	**ГОСТ 34.310:1995**	**ДСТУ ISO/IEC 14888-1:2002** ***Рандомізований механізм із детермінованим доказом***	**Відповідність**
Крок 1	Обчислення *h(M)* – значення геш-функції *h* від повідомлення *M*	Виконання попереднього підпису: Створення рандомізатора *K* Обчислення попереднього підпису (необов'язково)	+
Крок 2	Формування цілого числа *k* (є секретним і формується під час підпису повідомлення)	Підготовка повідомлення (з повідомлення *M* беруть дві частини M_1 і M_2, з яких можна відновити повне повідомлення *M*)	+
Крок 3	Обчислення двох значень: $r = a^k (\mathrm{mod}\ p)$ і $r' = r\ (\mathrm{mod}\ q)$	Обчислення доказу: геш-атрибут *H* від повідомлення *M*	+
Крок 3 (доповнення)	Якщо $r' = 0$, перейти до кроку 2 і створити інше значення числа *k*.	–	–
Крок 4	Обчислення геша повідомлення з використанням особистого ключа *x*	Обчислення підпису. Входами є рандомізатор *K*, ключ підпису *X*, детермінований доказ *H* і попередній підпис *П*	+
Підпис повідомлення	вектор $<r'>_{256} \| \| <s>_{256}$	Повний підпис має одну частину *S* або дві частини *R* та *S*	+

Таблиця 6. **Аналіз алгоритмів формування й верифікації підпису в ДСТУ 4145-2002 та ISO/IEC 14888:2008**

ДСТУ 4145-2002	**ISO/IEC 14888:2008**	**Аналіз відповідності й коментарі**
Формування цифрового підпису		
$Q = -dP$	Y = [X]G, де X – особистий ключ, G – точка на еліптичній кривій	+ Реалізація цього кроку в ISO/IEC 14888:2008 повністю відповідає ДСТУ 4145-2002
$h = \pi(H(M))$	Обчислення геш-коду. Якщо довжина вибраної геш-функції перевищує $log_2 q$, *H* встановлюється до крайнього лівого $log_2 q$ біту геш-коду від повідомлення $h(M_2)$. Інакше *H* – це $h(M_2)$. $(T_1, T_2) – (-R, -BS2I(H))$	– У ДСТУ 4145-2002 обчислення геш-коду відбувається на основі відкритого повідомлення $M : h = H(M)$
$R = eP$, $y = h\lambda(R) = hx_R$, $r = \vartheta(y) \mathrm{mod} n$	$\Pi = [K]G$, $R = FE2I(\Pi_x) \bmod q$	– В ISO/IEC 14888:2008 і ДСТУ 4145-2002 значення попереднього підпису обчислюють за однаковими показниками й технологією обчислення, зокрема як базової точки на еліптичній кривій і цілого числа, проте в ISO/IEC 14888:2008 відсутній крок обчислення елемента скінченного поля виду $\pi(h)x_R$ й перетворення його на велике ціле число, як це реалізовано в ДСТУ 4145-2002
$s = (e + dr) \mathrm{mod} n$	$S = (K^{-1}(XR + H)) \bmod q$ Якщо R=0 або S=0, треба згенерувати нове значення секретного цілого числа	– На відміну від ДСТУ 4145-2002 в ISO/IEC 14888:2008 передбачено варіант повторного створення цілого секретного числа, якщо R = 0 або S = 0
–	Формування доповнення як конкатенації (R, S) і поля тексту, тексту ((R, S), текст)	На відміну від ДСТУ 4145-2002 ISO/IEC 14888:2008 включає процедуру формування доповнення
$DS = \{0 \| r \| 0 \| s\}$	M||((R, S), текст)	– В ISO/IEC 14888:2008 формується підпис з доповненням, тому окремо додається текст до (R, S), де повідомлення M є конкатенацією (R, S), адже в ДСТУ 4145-2002 обчислюємо перетворення пари цілих чисел $\{s, r\}$ на цифровий підпис виду $DS = \{0 \| s \| 0 \| r\}$
Верифікація ЕЦП		
$h' = \pi(H(M))$	Верифікатор обчислює M від підписаного повідомлення і ділить повідомлення на дві частини M_1 і M_2. Повідомлення M_1 буде пустим, а M_2=M	– В ISO/IEC 14888:2008 реалізовано варіант розподілу повідомлення на дві частини, які є надійним кроком у верифікації підпису

Продовження табл. 6

ДСТУ 4145-2002	ISO/IEC 14888:2008	Аналіз відповідності й коментарі
$\{0 \| r \| 0 \| s\} = DS$	Відновлення доказу R і другої частини повідомлення S з доповненням. Перевірити наступне: $0 < R < q$ and $0 < S < q$ Якщо ці умови не виконано, повідомлення визнають недійсним	+
–	Assignment $T=(T_1, T_2)$ обчислюють як значення результату (-R, -BS2I(H)), де -BS2I є правилом конверсії для перетворення H на змінну	–
$r' = sP + rQ$, $y = h'\lambda(R') = h'x_R$, $r' = \vartheta(y) \bmod n$	$\bar{\Pi} = [-S^{-1} T_1 \bmod q]Y + [-S^{-1} T_2 \bmod q]G$ Повторно обчислюємо: $R = FE2I(\bar{\Pi}_x) \bmod q$ Вхідним є $\bar{\Pi}$, на виході одержимо результат $\bar{R}$	+/– Загалом кроки обчислення попереднього підпису є схожими, адже використано пару повідомлення (R, S), значення базової точки еліптичної кривої P (ДСТУ 4145-2002) або G (ISO/IEC 14888:2008) і значення відкритого ключа. Наголошуємо, що в ISO/IEC 14888:2008 використано значення $T=(T_1, T_2)$, що впливає на результат обчислення та бере участь в формуванні геш-коду. Більш того, в ISO/IEC 14888:2008 відбувається повторне обчислення доказу R, алгоритму, обчислення якого немає у ДСТУ 4145-2002
Якщо $r \equiv r'$, то цифровий підпис є валідний	Якщо $r \equiv r'$, то цифровий підпис є валідний	+ Специфіка ISO/IEC 14888:2008 Порівняння відбувається саме для R із кроку відновлення доказу R і другої частини повідомлення S із доповнення, де верифікуємо таке: $0 < R < q$ & $0 < S < q$, також $\bar{R}$ отримано на попередньому кроці

Порядок кроків підписування, вказаний в [4], несуттєво відрізняється. Зазначимо, що [4] для обчислення двох значень $r = ak \pmod p$ і $r' = r \pmod q$, якщо $r' = 0$, необхідно перейти до кроку формування секретного цілого числа й створити інше значення числа k, у [8] ця процедура не виконується. Алгоритми ідентичні.

Аналіз алгоритмів підпису ДСТУ 4145 та ISO/IEC 14888:2008. У таб. 6 відображено результати аналізу цифрового підпису згідно з [11] і [8].

Згідно з ДСТУ 4145-2002 використовують еліптичні криві над розширеним полем Галуа $GF(2^m)$, а в ISO/IEC 14888:2008 – $GF(p)$, де p – просте число.

Розглянемо поле $GF(p)$ як поле Галуа, на якому будують ЕЦП в ISO/IEC 14888:2008. Дві сторони інформаційного обміну A та B обирають спільне просте скінченне поле $GF(p)$, де p – велике просте число, домовляються про спільний породжувальний елемент g мультиплікативної групи цього поля, а потім кожна сторона вибирає свій приватний ключ (відповідно xA та xB), обчислюють відкритий ключ (відповідно до $y_A = g^{x_A}$, $y_B = g^{x_B}$, обчислення відбуваються в полі $GF(p)$, тобто за модулем простого числа p) та обмінюються відкритими ключами. Після цього спільний ключ K обчислюють як $K = (y_A)^{x_B} = \left(g^{x_A}\right)^{x_B} = g^{x_A x_B} = \left(g^{x_B}\right)^{x_A} = (y_B)^{x_A}$. Отже, задача типу $y = g^x$ зводиться до задачі дискретного логарифмування. У ДСТУ 4145-2002 поля використовують інакше. Терміни та визначення, застосовані в ДСТУ 4145 для формування ЕЦП, див. в табл. 7.

Таблиця 7. **Терміни ДСТУ 4145-2002**

ДСТУ 4145-2002	Визначення
Просте поле; GF(2)	Поле, що містить два елементи: 0 і 1
Основне поле	Скінченне поле $GF(2^m)$, яке є розширенням ступеня m поля GF(2). За визначенням це поле має характеристику 2. Допустимі значення ступеня m поля визначає стандарт ДСТУ 4145
Поліноміальний базис основного поля	Базис основного поля утворюють елементи (xm-1,..., x, 1) основного поля, де x – корінь примітивного багаточлена $f(t)$. Поліноміальний базис у цьому стандарті задають примітивний тричлен або п'ятичлен і корінь x
Нормальний базис основного поля	Базис основного поля (x, $x2$,..., $x^{2^{m-1}}$) утворено належно вибраним елементом x основного поля
Гаусівський оптимальний нормальний базис типу 2; оптимальний нормальний базис	Такий нормальний базис, що число $p'=2m+1$ є просте, а для такого найменшого натурального числа k, що $2k \equiv 1 \bmod(p')$, виконується одна з умов: а) $k = 2m$; б) $p' \equiv 3 \bmod 4$ і $k=m$

Еліптичною кривою E над полем $F = (F, +, \cdot)$ називають криву, визначену рівнянням (1):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (1)$$

де $a_i \in F$ (i=1,2,3,4,6) та містить нескінченну віддалену точку, позначену O.

Група точок еліптичної кривої, визначеної над скінченним полем, має такі властивості.

Групова операція досить проста, це вірно тільки для еліптичних кривих, визначених над скінченним полем характеристики 2, використання поля GF(p) для достатньо великого простого цілого p не надає жодних переваг і тому використовують еліптичні криві над полем GF(2^m), яке застосовано у ДСТУ 4145-2002 і називається базовим полем.

Якщо крива визначена над скінченним полем GF(2^m), то алгебраїчно замкнуте поле, що містить всі точки еліптичної кривої, є об'єднанням всіх розширень цього скінченного поля, тобто $\overline{K} = \bigcup_{k \geq 1} GF(2^{km})$. Зазначимо, коли коефіцієнти рівняння, що визначають еліптичну криву, належать основному полю, вона містить нескінченне число точок, а алгоритми будуються на скінченній кривій, координати точок якої належать основному полю. Отже, досягається складність повного перебору на актуальній нескінченності.

У таблиці 8 наведено відповідність між параметрами криптоалгоритмів у простому скінченному полі та полі характеристики 2 еліптичних кривих.

Стандарт є унікальним за структурою та даними, які він використовує [3]. Його [3] неможливо «згорнути» до будь-якого алгоритму [11], а необхідно вивести на міжнародний рівень як один із надійних алгоритмів підписування та почати роботу з його профілювання.

Висновки

Досягнення інтероперабельності НСЕЦП можливо лише за умови створення Технічного регламенту та впровадження трьох складових НСЕЦП: (1) політики підписування, (2) профілів та (3) комплектів підписування. Наслідки впровадження комплектів підпису висвітлено в цій статті. Зазначимо, що інтероперабельність реалізованих складових комплектів підпису гарантує процедура акредитації ЦСК, насамперед верифікація на тестовому стенді, на підставі якої до НСЕЦП допускаються тільки інтероперабельні програмно-технічні комплекси ЦСК. Важливо мати механізми гарантії стійкості комплектів підпису для безпеки ІТ, оскільки найслабша складова комплекту встановлюватиме загальний рівень надійності. У [1] введено поняття стійкості й наведено конкретні кількісні оцінки стійкості комплектів підпису.

Таблиця 8. **Відповідність між параметрами криптоалгоритмів**

Криптоалгоритм у простому скінченному полі	**Криптоалгоритм на еліптичній кривій над полем характеристики 2**
Циклічна підгрупа мультиплікативної (циклічної) групи простого скінченного поля GF(p) порядку u (u є дільник порядку мультиплікативної групи поля p-1)	Циклічна підгрупа порядку u групи (не обов'язково циклічної) точок еліптичної кривої над полем GF(2^m) (u – дільник порядку кривої N)
Породжувальний елемент циклічної підгрупи – ціле число g порядку u	Точка P циклічної підгрупи порядку u
Приватний ключ як ціле число t (з інтервалу (1, u-1)	Приватний ключ як ціле число t (з інтервалу (1, u-1)
Відкритий ключ як ціле число $y=g \bullet t$	Відкритий ключ як точка еліптичної кривої $Q=t$P

Впровадження [1] надасть змогу підвищити інтероперабельність НСЕЦП і гарантувати належний рівень безпеки ІТ. Тенденція широкого застосування міжнародних стандартів має стати основоположною для розвитку ІТ в Україні. Кінцеві користувачі повинні отримувати якісні послуги НСЕЦП за свої кошти. Зазначимо, що згідно з ЗУ «Про електронний цифровий підпис» держава гарантує якість послуг, які надаються.

Згідно з [1] і сукупністю ДСТУ в Україні чинні алгоритми підписування DSA, ECDSA, ECGDSA, RSA; геш-функції SHA-256, SHA-512, WHIRPOOL, але на підставі [5] їх не можна застосовувати у НСЕЦП. Для досягнення кроссертифікації й інтероперабельності НСЕЦП слід негайно переглянути [5] і розробити Технічний регламент НСЕЦП, оскільки вже зараз маємо базу з понад 50 чинних ДСТУ щодо ЕЦП.

1. ДСТУ ETSI TR 102 045 (V1.1.1) (2003-03) Електронні підписи й інфраструктури (ESI). Політика підписів для розширеної бізнес-моделі.
2. ДСТУ ETSI TS 102 176-1 (V2.0.0) (2007-11) Електронні підписи й інфраструктури (ESI); Алгоритми та параметри безпечних електронних підписів. Частина 1. Геш-функції й асиметричні алгоритми.
3. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевіряння.
4. ГОСТ 34.310-95 Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
5. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ та Держдепартаменту з питань зв'язку та інформатизації Мінтрансу від 11.09.2006 №99/166.
6. Закон України «Про стандартизацію» від 11.01.2006 № 2408-14.

7. ДСТУ ISO/IEC 13888-2002 Інформаційні технології. Методи захисту. Неспростовність (У 2-х частинах).
8. ДСТУ ISO/IEC 14888-2002 Інформаційні технології. Методи захисту. Цифрові підписи з доповненням (У 3-х частинах).
9. ДСТУ ISO/IEC 10118-2004 Методи захисту. Геш-функції (У 3-х частинах).
10. ДСТУ ETSI TS 101 862 (V1.3.3) (2006-01) Профіль посилених сертифікатів.
11. ISO/IEC 14888:2008 Information technology – Security techniques – Digital signatures with appendix (У 3-х частинах).

A. Melashchenko, O. Perevozchikova, O. Skarlat, K. Krivoruchko

SIGNATURE SUITES FOR INTEROPERABILITY OF NATIONAL SYSTEM OF ELECTRONIC DIGITAL SIGNATURES

In article possibilities of backward compatibility of current signature algorithm and hash functions in modified interoperable, with possibility of crosscertification National system of electronic digital signatures of Ukraine are analyzed. Also conformity listed in DSTU ETSI TS 102 176-1 standards with harmonized DSTU is resulted.

УДК 519.8

Чечельницький О. А., Франчук О. В., Кирієнко О. В.

ГРАНИЧНІ ХАРАКТЕРИСТИКИ МОДЕЛІ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТИПУ ДЖЕКСОНА

В роботі досліджено граничні характеристики математичної моделі комп'ютерної мережі типу Джексона з двовимірним пуассонівським потоком вимог.

1. Опис моделі

У різних сферах нашого життя дедалі частіше значну роль відіграють комп'ютерні мережі. Будь-яка мережа складається з певної кількості функціонуючих елементів, які звичайно називають вузлами мережі. Вузли взаємодіють між собою. Задачею вузлів є обробка вимог (завдань), які надходять ззовні. Дуже часто завдання надходить не для одного вузла, а відразу для декількох, або навіть для всіх вузлів мережі. Ось чому велике значення має аналіз властивостей математичних моделей мережевих структур з відповідними вхідними потоками.

У цій статті ми розглянемо модель мережі Джексона, елементами якої є системи масового обслуговування типу $M/M/\infty$ з двовимірним пуассонівським вхідним потоком вимог $\left(\nu_1(t),\nu_2(t)\right)$ з параметрами $\lambda_1>0$, $\lambda_2>0$, $b>0$. Вимоги з потоку $\nu_1(t)$ на першу систему, а вимоги з потоку $\nu_2(t)$ – на другу систему обслуговування. Нехай $\mu_i>0, i=1,2$ параметри показникових розподілів часу обслуговування відповідно в першій та другій системі. Позначимо також через $X_1(t)$ число вимог, які обслуговуються в першій системі $M/M/\infty$ в момент часу t, а через $X_2(t)$ – число вимог у другій системі в момент часу t. Після обслуговування в першому вузлі вимога з ймовірністю p_{12} надходить на обслуговування до другої системи, або з ймовірністю p_{13} залишає нашу мережу. Аналогічно, після обслуговування в другому вузлі вимога з ймовірністю p_{21} переходить на обслуговування до першого вузла, або з ймовірністю p_{23} залишає мережу.

Однією з ключових проблем, яка розв'язується в рамках теорії масового обслуговування, є дослідження стаціонарних характеристик моделі. Очевидно, що найбільш успішним на цьому шляху є випадки, коли вдається знайти стаціонарний розподіл процесу обслуговування $\left(X_1(t),X_2(t)\right)$. Тому актуальною стає наступна теорема.

Теорема 1. Нехай мережа Джексона $(M/M/\infty)^2$ є відкритою, тобто хоча б для одного індексу