УДК 004 056 55

ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ С ИСПОЛЬЗОВАНИЕМ КРИПТОСИСТЕМ NTRU

Д.С. БАЛАГУРА, И.А. БАГЛАЕВ

Проводится исследование функционала инфраструктур открытых ключей в части использования криптографических протоколов. Определяется возможность использования криптосистем NTRU в инфраструктурах открытых ключей.

Ключевые слова: инфраструктуры открытых ключей, несимметричные криптосистемы, криптосистема NTRU, сертификат, личный ключ.

Инфраструктуры открытых ключей предназначены для управления ключевыми данными в различных, зачастую открытых информационных структурах. В таких случаях необходимо использовать несимметрические алгоритмы, кроме того, эти же алгоритмы зачастую используются и в элементах управления инфраструктурами открытых ключей. Таким образом, можно сказать, что функционирование инфраструктур открытых ключей напрямую зависит от выбора алгоритмов цифровой подписи и направленного шифрования. В данной работе представлен перспективный алгоритм шифрования и цифровой подписи NTRU, основанный на преобразования в кольцах усечённых полиномов, который может заменить действующие алгоритмы RSA, DSA, ECDSA и им подобные. Подробное описание всех этих алгоритмов и криптосистем можно найти в большом количестве различных источников [1, 2].

1. ВОЗМОЖНОСТЬ ИСПОЛЬЗОВАНИЯ NTRU В ИНФРАСТРУКТУРАХ ОТКРЫТЫХ КЛЮЧЕЙ

Основываясь на описании, анализе, требованиях, которые предъявляются к инфраструктурам открытых ключей в мире в целом и в Украине в частности, рассмотрим возможность использования в них NTRU криптосистем.

Как известно, инфраструктуры открытых ключей строятся и эксплуатируются для обеспечения конечных пользователей аутентичными и целостными копиями открытых ключей других пользователей (сертификатами открытых ключей). Исходя из назначения и задач инфраструктуры открытых ключей, в ней формируются центры сертификации ключей (ЦСК). Основными криптографическими операциями, использующимися ЦСК, являются операции цифровой подписи, а также направленного шифрования и симметрического шифрования. Естественно, использование симметрических алгоритмов и хеш-функций не зависит от используемых алгоритмов ЭЦП и направленного шифрования (кроме аспектов, связанных с общей стойкостью системы). Рассмотрим основные протоколы (действия) инфраструктур открытых ключей и алгоритмы, применяемые в них.

а) протокол отправки ключа на сертификацию/получения сертификата. В зависимости от класса системы и требований, предъявляемых к её защищённости, возможно использование ЭЦП и направленного шифрования;

б) сертификация открытого ключа ЦСК, серверов ЦСК, открытых ключей пользователей. Используется ЭЦП;

в) формирование списков отозванных сертификатов. Используется ЭЦП;

г) формирование меток времени. Используется ЭЦП;

д) формирование ответов на запросы по протоколу OCSP. Используется ЭЦП;

е) использование ключей и сертификатов конечными пользователями:

– цифровая подпись;

– направленное шифрование.

Таким образом, в протоколах инфраструктур открытых ключей из несимметричных алгоритмов используются алгоритмы электронной цифровой подписи и направленного шифрования. Учитывая тот факт, что криптосистемы на базе NTRU позволяют реализовывать как направленное шифрование, так и электронную цифровую подпись, то существует возможность построения инфраструктуры открытых ключей, которая будет полностью основываться на криптосистеме NTRU.

В последующих разделах рассматриваются различные аспекты построения инфраструктур открытых ключей с использованием NTRU, а также проводится сравнение протоколов ИОК, основывающихся на RSA, эллиптических кривых и NTRU [3, 4].

2. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ПРОТОКОЛОВ ИНФРАСТРУКТУР ОТКРЫТЫХ КЛЮЧЕЙ С ИСПОЛЬЗОВАНИЕМ NTRU

Протоколы управления сертификатами инфраструктуры открытых ключей требуются для обеспечения целостности, конфиденциальности, неотказуемости, подтверждения авторства, а также поддержки on-line взаимодействия между компонентами PKI.

Рассматриваемые протоколы должны удовлетворять следующим требованиям к управлению PKI[2]:

Управление PKI должно соответствовать стандарту ISO 9594-8 и связанным с ним расширениям сертификата.

Управление PKI должно соответствовать стандарту X.509 v3.

Должна быть возможность регулярного изменения любой пары ключей без влияния на какую-либо другую пару ключей.

Использование сервисов, обеспечивающих конфиденциальность, в протоколах управления PKI должно быть сведено к минимуму, чтобы уменьшить связанные с этим проблемы.

Протоколы управления PKI должны допускать использование различных криптографических алгоритмов, являющихся промышленными стандартами (специально включая только RSA, DSA, MD5, SHA-1). Это означает, что центры регистрации/сертификации или конечный пользователь PKI могут использовать для своей пары ключей любой набор алгоритмов.

Протоколы управления PKI должны поддерживать опубликование сертификатов, относящихся к конечным пользователям, центрам сертификации/регистрации.

Протоколы управления PKI должны поддерживать создание списков отозванных сертификатов, позволяя сертифицированным конечным пользователям посылать запросы на отмену сертификатов – это должно быть организовано так, чтобы невозможно было предпринять DoS-атаку.

Протоколы управления PKI должны использоваться поверх различных транспортных механизмов, включая LDAP, SMTP, HTTP, TCP/IP и FTP.

При запросе конечным пользователем сертификата, содержащего данное значение открытого ключа, конечный пользователь должен быть готов продемонстрировать обладание соответствующим значением закрытого ключа. Это можно организовать по-разному, в зависимости от типа алгоритма открытого ключа.

В зависимости от топологии ИОК, а также использования алгоритмов NTRU, возможны некоторые изменения в выдвигаемых требованиях. В табл. 1 приведены основные протоколы, использующие NTRU шифрование и цифровую подпись.

3. СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ PKI, С ИСПОЛЬЗОВАНИЕМ РАЗЛИЧНЫХ КРИПТОСИСТЕМ

Как отмечалось ранее, криптосистема NTRU имеет некоторые преимущества, по сравнению с такими криптосистемами как RSA, DSA, EGSA, ECDSA и им подобным:

1. Процедура направленного зашифрования/расшифрования и подписи более эффективна как на программной, так и на аппаратной реализации.

Таблица 1

Основные протоколы ИОК, с использованием NTRU

Протоколы (действия)	NTRUEncrypt	NTRUSign
Отправка ключа на сертификацию Получение сертификата	+	+
Сертификация ключа ЦСК Сертификация конечных пользователей	+/-	+
Формирование CAC	-	+
Формирование меток времени	+/-	+
Формирование ответов на запросы (OCSP)	-	+
Использование ключей и сертификатов конечных пользователей	+	+

2. Процедура генерации ключа происходит гораздо быстрее, что позволяет использовать сеансовые ключи.

При равных длинах ключа, стойкость NTRU выше, чем стойкость RSA.

Сравнение стойкости основных ассиметричных систем.

Предварительная безопасность и временные сравнения NTRU и RSA представлены в табл. 2. RSA и NTRU работают в единицу времени на блок сообщения. Таким образом, в таблице 2 представлены значения времени зашифрования/расшифрования единичного блока сообщения [3].

Таблица 2

Сравнение RSA и NTRU

Система	Безопасность (MIPS за год)	Длина ключа (бит)	Генерация ключа (мс)	Шифрование (блок/с)	Расшифрование (блок/с)
RSA 512	$4{,}00 \cdot 10^{5}$	512	360	2441	122
NTRU 167	$2{,}08 \cdot 10^{6}$	1169	4.0	5941	2818
RSA 1024	$3{,}00 \cdot 10^{12}$	1024	1280	932	22
NTRU 263	$4{,}61 \cdot 10^{14}$	1841	7.5	3676	1619
RSA 2048	$3{,}00 \cdot 10^{21}$	2048	4195	310	3
RSA 4096	$2{,}00 \cdot 10^{33}$	4096	-	-	-
NTRU 503	$3{,}38 \cdot 10^{35}$	4024	17.3	1471	608

Однако NTRU имеет недостатки, связанные с выбором параметров и проверкой подписи:

1. Необходимость использования только рекомендованных параметров (табл. 3).

2. Вероятность возникновения ошибки при проверке подписи. Даже верно сформированная подпись не всегда пройдёт проверку.

3. Размер подписи варьируется.

Таблица 3

Рекомендуемые параметры NTRU

	N	p	q	d_f	d_g	d_r
NTRU167:3	167	3	128	61	20	18
NTRU251:3	251	3	128	50	24	16
NTRU503:3	503	3	256	216	72	55
NTRU167:2	167	2	127	45	35	18
NTRU251:2	251	2	127	35	35	22
NTRU503:2	503	2	253	155	100	65

Сравнение производительности ассиметричных алгоритмов

Табл. 4 содержит набор параметров с соответствующим для них уровнем безопасности, производительность (с точки зрения подписания/проверки подписи за секунду) для каждого из рекомендованного набора параметров.

Для уровня безопасности больше чем 80 бит, длина подписи NTRU меньше чем соответствующая RSA подпись, однако больше чем ECDSA. Секретный ключ NTRUSign содержит в себе полиномы f и g, а так же полиномы f_i, g_i и h_i. Для хранения полиномов f и g необходимо $2N$ бит, а для полинома h необходимо $N\log_2(q)$ бит. Таким образом, для параметров размером 80–128 бит необходимо $16N$ бит для хранения ключевых данных и $17N$ бит для параметров размером в 160–256 бит, что примерно в два раза больше чем длина открытого ключа.[4]

ВЫВОДЫ

Функционирующие инфраструктуры открытых ключей могут использовать различные несимметричные алгоритмы направленного шифрования и цифровой подписи. В зависимости от масштаба и топологии ИОК, выбирают те или иные алгоритмы, исходя из требований стойкости, скорости работы и т.д. В проделанной работе была рассмотрена перспективная несимметричная криптосистема NTRU, которая имеет как преимущества, так и недостатки.

В первую очередь, стоит отметить, что криптосистема NTRU отличается от остальных криптосистем математическим аппаратом и основана на алгебраической структуре полиномиального кольца, что позволяет выполнять процедуры шифрования, подписи и проверки подписи гораздо быстрее, чем алгоритм RSA. В то время как RSA с длиной ключа в 512 бит шифрует примерно 2441 блоков/с и создаёт 824 подписи/с, NTRU:167 шифрует 5941 блок/с и создаёт 13841 подпись/с. Эти данные свидетельствуют о высокой скорости работы алгоритма. При определённых наборах параметров NTRU и ECDSA, обеспечивающих примерно равную стойкость, криптосистема NTRU работает немного быстрее, чем криптосистема на эллиптических кривых. Вдобавок к этому, процедура генерации ключа происходит гораздо быстрее, чем в других криптосистемах, что позволяет использовать «одноразовые» ключи.

Важным моментом является относительно большая размерность ключа и общесистемных параметров, что, безусловно, приведёт к увеличению размера цифрового сертификата в целом.

В данный момент не существует инфраструктур открытых ключей, функционирующих с использованием криптосистемы NTRU. Одной из причин этому является проблема при подписании сообщения и соответственно при проверке подписи. Данные нюансы ставят под сомнение использование криптосистемы NTRU в инфраструктурах большого масштаба. Однако, дальнейшие исследования по нахождению определённых константных значений, исключающих или уменьшающих вероятность появления ошибки при проверке подписи, позволяют предположить, что криптосистема NTRU найдёт широкое применение в инфраструктурах открытых ключей.

Литература

[1] Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика *Ю.І. Горбенко, І.Д. Горбенко.* – Харків «Форт», 2010. – 608 с.

[2] Основы технологии PKI. *В.С. Горбатов, О.Ю. Полянская.* – М.:Горячая линия – Телеком, 2004. – 248 с.

[3] NTRU: A public key cryptosystem *J. Hoffstein, D. Lieman, J. Pipher, Joseph H. Silverman.* – M., 2004 – 17 с.

[4] Practical lattice-based cryptography: NTRUEncrypt and NTRUSign *J. Hoffstein, N. Howgrave-Graham, J. Pipher, W. Whyte.* – M., 2005. – 42 с.

Поступила в редколлегию 14.05.2013

Таблица 4

Производительность NTRUSign для различных наборов параметров

Параметры				Открытый ключ и размер подписи				Подписей/с			Проверок/с		
k	N	d	q	NTRU	ECDSA ключ	ECDSA подпись	RSA	NTRU	ECDSA		NTRU	ECDSA	
80	157	29	256	1256	192	384	1024	4560	5140	0.89	15955	1349	11.83
112	197	28	256	1576	224	448	~2048	3466	3327	1.04	10133	883	11.48
128	223	32	256	1784	256	512	3072	2691	2093	1.28	7908	547	14.46
160	263	45	512	2367	320	640	4096	1722	-	-	5686	-	-
192	313	50	512	2817	384	768	7680	1276	752	1.69	4014	170	23.61
256	349	75	512	3141	512	1024	15360	833	436	1.91	3229	100	32.29

Балагура Дмитрий Сергеевич, фото и сведения об авторе см. на стр. 257.

Баглаев Игорь Алексеевич, студент кафедры Безопасности информационных технологий ХНУРЭ. Научные интересы: защита информации, инфраструктуры открытых ключей.

УДК 004 056 55

Інфраструктури відкритих ключів з використанням криптосистем NTRU / Д.С. Балагура, І.О. Баглаєв // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 299–302.

Здійснюється дослідження функціоналу інфраструктур відкритих ключів у частині використання криптографічних протоколів. Визначається можливість використання криптосистем NTRU в інфраструктурах відкритих ключів.

Ключові слова: інфраструктури відкритих ключів, несиметричні криптосистеми, криптосистема NTRU, сертифікат, особистий ключ.

Табл.: 4. Бібліогр.: 4 найм.

UDC 004 056 55

Public key infrastructures with the use of NTRU cryptosystems / Balagura D.S., Baglaev I.A. // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 299–302.

Research of the functional of public key infrastructures regarding the use of cryptographic protocols is conducted. A possibility of using NTRU cryptosystems in public key infrastructures is defined.

Keywords: public key infrastructures, asymmetrical cryptosystems, NTRU cryptosystem, certificate, personal key.

Tab.: 4. Ref.: 4 items.