Порівняйте відомі вам стандарти НШ по критеріям стійкості та складності перетворень для застосування в протоколі «захищені дані», які переваги вони мають один перед іншим

Таблиця 12.12 — Порівняння швидкостей NTRU, RSA и ЭК

Уровень стойкости(біт БСШ)	Операций/секунда		
	NTRU	ЭК	RSA
112	10638	951	156
128	9901	650	12
192	6849	285	8
256	5000	116	1

Таблиця 12.13 - Асиметричні криптографічні перетворення для реалізації направленого шифрування

Параметри НШ/ Математичний апарат	Особистий ключ НРШ	Відкритий ключ НЗШ (сертифікат)	Асиметрична пара (ключ)	Загальні параметри крипто перетворення	Сертифікати	Складність крипто аналізу
НШ в кільці (RSA)	D_i	E_i	(D_i , E_i)	$N = P\ Q$	E_i	Субекспоненційна
НШ в полі Галуа $F(P)$	X_i	$Y_i=g^{X}{}_i(\text{mod } P)$	(X_i, Y_i)	P, q, g	Y_i	Субекспоненційна

НШ в групі точок еліптичних кривих $E(F(q))$	d_i	$Q_i=d_i G(\mathrm{mod} q)$	(d_i, Q_i)	$a, b, G, n, f(x)(P), h$	Q_i	Експоненційна
НШ в гіпереліптичних кривих	C_i	$D_2= c_i D_1$	(c_i, D_2)	$f(x), g(x), q, D_1, g, J$	D_2	Експоненційна
НШ зі спарюванням точок еліптичних кривих	$d_{iD} = s\ Q_{iD}$	$Q_{iD}=H_1(ID)$	(d_{iD}, Q_{iD})	$G_1, G_2, e, H_1, P, H_2, H_3, F_2^m, P_p$	Q_{iD}	Експоненційна – субекспоненційна
НШ в кільці зрізаних поліномів (NTRU)	$f = 1+pF$ (modq)	$h=$ f ^{1}*g*p(modq)	(f, h)	N, q, p, f, g, df, dg, c		Експоненційна – субекспоненційна

Таблиця 12.14

Порівняння стійкості стандартизованих асиметричних крипто перетворень

Рівень стійкості, в бітах	Симетричні	Оцінка часу крипто аналізу, MIPS-years	Геш функції	Параметри асиметричних перетворень				
				DSA	RSA	EC-DSA	IBE (BF, BB1)	NTRU
До 2010 р. (мін. 80 біт стійкості)	2TDEA 3TDEA AES-128 AES-192 AES-256	10^9	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Min.: L = 1024; N =160	Min.: k=1024	Min.: f=160	Min.: p = 512 q = 160	N =263 q =2048 d_f = 113
До 2030 р. (мін. 112 біт стійкості)	3TDEA AES-128 AES-192	10^{17}	SHA-224, SHA-256, SHA-384,	Min.: L = 2048 N = 224	Min.: k=2048	Min.: f=224	Min.: p = 1024 q = 224	N =401 q =2048 d_f = 113

	AES-256		SHA-512					
Після 2030 (мін. 128 біт стійкості)	AES-128 AES-192 AES-256	10^{23}	SHA-256, SHA-384, SHA-512	Min.: L = 3072 N = 256	Min.: k=3072	Min.: f=256	Min.: p = 1536 q = 256	N =449 q =2048 d_f = 134
Рівень стійкості 192 біта	AES-192 AES-256	10^{41}	SHA-384, SHA-512	Min.: L = 7680 N = 384	Min.: k=7680	Min.: f=384	Min.: p = 3840 q = 384	N =677 q =2048 d_f = 153
Рівень стійкості 256 біта	AES-256	10^{63}	SHA-512	Min.: L = 15360 N = 512	Min.: k=15360	Min.: f=512	Min.: p = 7680 q = 512	N =1087 q =2048 d_f = 120