SIDH/Isogeny Signature Function Contracts

Robert Gorrie – McMaster University – November 28, 2017

1 Key Exchange

1.1 Ephemeral Key Generation – Alice

Key Generation for Alice

Location	Efficient Algo's Appendix A
Input	$x_{P_B}, x_{P_A}, y_{P_A}$, $SK_{Alice} = m_A \cdot l_A$
Output	$PK_{Alice} = [x_{\Phi_A}(P_B), x_{\Phi_A}(Q_B), x_{\Phi_A}(Q_B - P_B)]$

EphemeralKeyGeneration_A

Location	kex.c
Input	unsigned char* PrivateKeyA, unsigned char* PublicKeyA, PCurveIsogenyStruct CurveIsogeny, invBatch* batch
Output	publickey_t PublicKeyA, digit_t PrivateKeyA

Key Generation for Alice

Location	Efficient Algo's Appendix A
Input	$x_{P_B}, x_{P_A}, y_{P_A}$, $SK_{Alice} = m_A \cdot l_A$
Output	$PK_{Alice} = [x_{\Phi_A}(P_B), x_{\Phi_A}(Q_B), x_{\Phi_A}(Q_B - P_B)]$

EphemeralKeyGeneration_A

Location	kex.c
Input	unsigned char* PrivateKeyA, unsigned char* PublicKeyA, PCurveIsogenyStruct CurveIsogeny, invBatch* batch
Output	publickey_t PublicKeyA, digit_t PrivateKeyA

1.2 Ephemeral Key Generation – Bob

1.3 Ephemeral Secret Agreement – Alice

1.4 Ephemeral Secret Agreement – Bob

2 Signature Scheme

2.1 Keygen

KeyGeneration_A

Location	kex.c
Input	unsigned char* PrivateKeyA, unsigned char* PublicKeyA, PCurveIsogenyStruct CurveIsogeny, invBatch* batch
Output	publickey_t PublicKeyA, digit_t PrivateKeyA

KeyGeneration_B

Location	kex.c
Input	unsigned char* PrivateKeyA, unsigned char* PublicKeyA, PCurveIsogenyStruct CurveIsogeny, invBatch* batch
Output	publickey_t PublicKeyA, digit_t PrivateKeyA

2.2 Sign

2.3 Verify

3 Elliptic Curve Operations

4 Field Operations

5 Type Definitions

alias	definition
digit_t	uint64_t
felm_t	digit_t[NWORDS_FIELD]
f2elm_t	felm_t[2]
publickey_t	f2elm_t[3]