AKE Zoo: 100 two-party protocols (to be continued)

Alekseev E.K.[1], Babueva A.A.[2], Zazykina O.A.[3]

Abstract

The problem of designing authenticated key establishment protocols has a rich history. Since 1976 more than a hundred different protocols have been proposed. But the task of comparing and classifying existing protocols is usually complicated by the fact that they are described in different terms and with different levels of detail. This paper contains intermediate results on enumeration and uniform description of AKE protocols. We publish it in order to get feedback on the description principles used. Here we describe 100 AKE protocols (there are much more such protocols, but we found these earlier) in identical terms and the same level of detail. The proposed descriptions are not structured (chronologically only) but classifying of these protocols is future work direction.

1 Introduction

This paper focuses on the enumeration and description of two-party authenticated key establishment (AKE) protocols, specifically those that use standard cryptographic primitives and basic group operations. We assume that these protocols result in both parties sharing a secret key. We describe AKE protocols uniformly, meaning that we present them at the same level of detail (see Section 2) and employ identical terms (see Section 3), to facilitate the determination of the cryptographic principles behind such protocols and evaluation of their security.

Here we present interim results comprising first 100 AKE protocols we found in the literature. There is no doubt that there are many more AKE protocols, and our goal for the final version of this paper is to describe as many of them as we can find. However, we exclude from the consideration identity-based AKE protocols (e.g. [56, 57]) as well as protocols that employ post-quantum or not widespread (at the time of publication of the paper) cryptographic techniques (e.g. [58, 59, 60, 61, 62]). Furthermore, we focus only on those protocols that were explicitly designed for the two-party case, where each party possesses either a key pair or a high-entropy common secret. Therefore, group protocols (e.g. [63, 64, 65]) modified for the two-party case, or PAKE protocols (e.g. [66, 67, 68]) in

[1]CryptoPro LLC, alekseev@cryptopro.ru
[2]CryptoPro LLC, babueva@cryptopro.ru
[3]MTUCI Moscow, zazykinaoa@gmail.com

a case where password is replaced by a high-entropy value will not be described. However, adding such protocols to the list given in this paper may be an interesting further research direction.

2 Principles of cryptographic core

An example of descriptions presented in this paper is the description of the Photuris protocol from [20]. Originally this protocol was described in the document [15], taking 76 pages. Such a detailed description is mainly intended for developers and is aimed at facilitating the creation of compatible implementations. However, this description is inconvenient for identifying the cryptographic properties of this protocol and comparing it with other protocols. The paper [20] describes the protocol that «used as the core cryptographic protocol in Photuris». Such a simplified description was enough for the authors of this paper to demonstrate the vulnerability of this «core» protocol and consequently the full Photuris protocol to the unknown key share threat.

Note that when we describe just the cryptographic core of a protocol we in some sense simplify it. This leads to the fact that some vulnerabilities of the original protocol might not longer be detected using the descriptions given in this paper. Therefore, in order to draw conclusions about the security of protocols used in practice, it is necessary, in addition to the properties of their cryptographic cores, also to take into account the details of their extended descriptions given in various standards and development specifications.

Further we describe in detail several principles that define what we call the cryptographic core in this paper.

1. **No PKI:** we don't describe details of the trusted distribution of public keys;
2. **Classes of cryptoprimitives:** we use terminology of classes of primitives, we don't fix any specific representatives;
3. **No formats:** we don't describe message formats in detail;
4. **No out-of-group elements:** the party always checks that the received element belongs to the group before any other calculations, and interrupts the protocol execution if the verification failed;
5. **Prime order groups:** we describe all group calculations for the case of a group of a prime order;
6. **Ordered messages:** we assume that protocol messages are sent strictly in the order specified in its description.

No PKI. Ensuring that public key pk_A belongs to the party with identifier A can be solved in various ways, for example, using public key certificates, and is not the task of the AKE protocols (a similar assumption is used, for example, in [20]). Therefore, in descriptions, a party always sends only its identifier to the other party. When clarifying a protocol for a specific practical application, the identifier can (and most likely will) be replaced, for example, with a public key certificate of the relevant party.

Classes of cryptoprimitives. In Section 3.1 we introduce classes of cryptographic primitives and corresponding notations to describe all protocols. So we don't use concrete representatives and generalize the description if it initially uses a specific cryptoprimitive (e.g. [51]). Separately, note how we use the KDF function. A number of protocols specify a concrete procedure for generating certain keys, for example, $\mathsf{H}(A) \oplus \mathsf{H}(B) \oplus \mathsf{H}(C)$ or $A + B + C$, where A, B, C are group elements computed earlier. So when key generation includes applying some cryptographic primitive and results in a binary string we describe it in a more general way $\mathsf{KDF}(A, B, C)$. In other cases (result is a group element, or procedure does not use any cryptographic primitives) we describe it directly: $A + B + C$ or $\nu(A) + \nu(B)$ as in mMQV-P1 description (see Section 5.14). Also we assume that the neutral element of the group cannot be a parameter of any cryptographic primitive. If this happens, the party interrupts the execution of the protocol with an error.

No formats. In our descriptions, we assume that all parts of the transmitted messages are clearly distinct and we omit the details of formatting messages (as stated in [54], «but in practice a principal receiving a message, whether encrypted or not, simply sees a string of bits which have to be interpreted»). In descriptions that are implementation-oriented, of course, message formats are usually described (e.g. [15]). Note, that this simplification does not allow to analyze these protocols for the applicability of the, so-called, «typing attacks» (see [54] or [73]).

No out-of-group elements. We assume that when an element of a group is received from a channel, it is first checked for belonging to this group, and only after some calculations are performed with it. Consequently, our descriptions do not define the procedure for performing such checks even if it is defined by the authors. This excludes the possibility of analyzing these protocols for the applicability of the invalid-curve attacks (see, for example, [70, 71]).

Prime order groups. We describe all protocols for the case of calculations in an additive group of prime order. This excludes the possibility of analyzing these protocols for the applicability of the small subgroup attacks (see, for example, [21, 69]).

Ordered messages. We provide descriptions of the protocols, assuming that the order of messages is fixed. That is, before receiving the first message from the party with

identifier A, the party with identifier B is in a standby mode and begins to perform any calculations only after it receives a message from the other party, which contains all expected values and only them. We mean that the parties carry out such correctness checks, but we do not specify them explicitly in the descriptions of protocols. After sending its message, a party waits for a new message from the other party, or performs the final calculations and returns the result of interaction. Note that the ordering of messages allows the parties, in addition to the common key, to determine their roles (initiator or responder) in the interaction, although they may not need them at the application level (examples of systems where roles are used at the application level are given in [72]). At the same time, some protocols are initially designed to be used (in particular, for optimization purposes) without ordering the messages (see, for example, [26, 27]). Note that such protocols can be naturally described and applied in conditions when messages are ordered.

3 Principles of uniform description

3.1 Notations

If an input of a function or algorithm, which is a binary string, consists of the values of several parameters, then we list these parameters separated by commas in parentheses. At the same time, we assume that each of the listed parameters is injectively translated from the set of possible values into a set of binary strings. Thus, based on the resulting value of the input argument, it is possible to unambiguously restore the values of the parameters from which it was obtained. If the function or algorithm has only one argument, then the second brackets will be omitted. So, for example, if f is a function of two arguments and g is a function of one argument, then we write $f((x_1, x_2), (y_1, y_2))$ and $f(x, (y, z))$, but $g(x, y)$.

Group calculations. Calculations in a group assumed by the original description of the protocol are described for the case of an additive group G of a prime order q. The generators of this group are denoted by P, P', P'' and so on. We denote by $\mathbb{Z}_q$ a finite field of characteristic q and assume the canonic representation of the elements in $\mathbb{Z}_q$ as integers in the interval $[1...q-1]$. We denote by $\mathbb{Z}_q^*$ the set $\mathbb{Z}_q$ without the zero element.

Keys. We use the following notations for cryptographic keys and shared non-secret values.

x, X	key pair consisting of a scalar x and corresponding multiple element of the group $X = x \cdot P$ which are used in group operations specified by the protocol itself (in the protocol description we always write x, X without specifying that $X = x \cdot P$)
(sk^s, pk^s)	key pair of a signature scheme (without specifying the nature of this values)
(sk^e, pk^e)	key pair of a public key encryption scheme (without specifying the nature of this values)
(sk^k, pk^k)	key pair of a key encapsulation mechanism is denoted by (sk^s, pk^s) (without specifying the nature of this values)
psk	long-term common secret value (Pre-Shared Key)
K^e	key of a symmetric encryption scheme
K^a	key of a message authentication scheme
K^{ae}	key of a authenticated encryption scheme
K^p	key of a pseudorandom function
K	shared secret key established as a result of the protocol, the corresponding key space is denoted by $\mathcal{K}$; in some descriptions it may also be used as the key of a symmetric encryption scheme and a message authentication scheme

Cryptoprimitives. We use the following notations for the classes of primitives.

$\mathcal{SIG}$	*signature scheme:* KGen — key generation algorithm $\mathsf{Sig}_{sk^s}(\cdot)$ — signing algorithm using the private key sk^s σ — signature value
$\mathcal{PKE}$	*public key encryption scheme:* KGen — key generation algorithm $\mathsf{Enc}_{pk^e}(\cdot)$ — encryption algorithm using the public key pk^e $\mathsf{Dec}_{sk^e}(\cdot)$ — decryption algorithm using the private key sk^e
$\mathcal{SE}$	*symmetric key encryption scheme:* KGen — key generation algorithm $\mathsf{Enc}_{K^e}(\cdot)$ — encryption algorithm using the symmetric secret key K^e $\mathsf{Dec}_{K^e}(\cdot)$ — decryption algorithm using the symmetric secret key K^e
$\mathcal{KEM}$	*key encapsulation mechanism:* KGen — key generation algorithm $\mathsf{Encaps}_{pk^k}(\cdot)$ — encapsulation algorithm using the public key pk^k; generally it may take as an input one argument associated with the randomness to be used, if there is no arguments it is assumed that the random values are chosen internally during the algorithm execution

	$\mathsf{Decaps}_{sk^k}(\cdot)$ — decapsulation algorithms using the private key sk^k
$\mathcal{AE}$	*authenticated encryption scheme:* KGen — key generation algorithm $\mathsf{Enc}_{K^{ae}}(\cdot,\cdot)$ — encryption algorithm using the symmetric secret key K^{ae}, the first parameter is an associated (unencrypted) data, and the second parameter is a plaintext $\mathsf{Dec}_{K^{ae}}(\cdot,\cdot)$ — decryption algorithm using the symmetric secret key K^{ae}, the first parameter is an associated (unencrypted) data, and the second parameter is a plaintext
$\mathcal{MAC}$	*message authentication scheme:* KGen — key generation algorithm $\mathsf{MAC}_{K^a}(\cdot)$ — algorithm for generating the message authentication code using the key K^a τ — message authentication code value
$\mathsf{PRF}_{K^p}(\cdot)$	*pseudorandom function* using the symmetric secret key K^p: if the protocol assumes the generation of a pseudorandom function key we write that the key is chosen uniformly at random from $\mathcal{K}_p$, where $\mathcal{K}_p$ denotes the corresponding message space
$\mathsf{KDF}(\cdot)$	*key derivation function:* generally it may take as an input an arbitrary number of arguments corresponding either to the input key material or to the context information, the length of output key material is not taken as an input and can be determined from the protocol description by the number of output keys
$\mathsf{H}(\cdot)$	*hash function:* depending on its usage in the protocol, we assume that hash values are binary strings of some fixed length or elements from $\mathbb{Z}_q$

If several primitives of the same type $\mathcal{M}$ are used in the protocol description, we denote them by $\mathcal{M}^i, i = 1, 2, \ldots$.

For brevity, in our descriptions we write Sig_{sk^s} and MAC_{K^a} instead of $\mathcal{SIG}.\mathsf{Sig}_{sk^s}$ and $\mathcal{MAC}.\mathsf{MAC}_{K^a}$ respectively.

Miscellanea. We also use the following additional notations.

λ	security parameter
μ	function from G to $\mathbb{Z}_q$
ν	function from G to $\{0,1\}^s$ for some s, which is determined from the context
$\mathsf{c}_1, \mathsf{c}_2, \mathsf{c}_3, \mathsf{c}_4$	various nonzero strings of the same length fixed within the protocol

ε	empty string
GetTime	function which returns the current time
$a \xleftarrow{\mathcal{U}} A$	element a is chosen from the set A uniformly at random
$a \oplus b$	bitwise addition modulo 2 of bit strings a and b of the same length

3.2 Protocol description

In the protocols described in this paper, there are always two parties, which are denoted by **A** and **B**, and **A** is the initiator, and **B** is the responder.

For convenience, when specifying the identifiers of the parties, we use the same notations as for the parties themselves, but in italics and without bold highlighting: A and B. We add a subscript with the identifier of one of the parties for values that are similar in meaning, but not equal in value (e.g. ephemeral keys E_A and E_B), but we use the same notation for the same values that coincide on both sides when the protocol is executed correctly (e.g. the result shared key K).

When describing a protocol, we first list long-term parameters of each party (e.g., $\mathbf{A} : x_A, X_A$ or $\mathbf{B} : (sk_B^s, pk_B^s), \mathsf{sid}, \mathsf{psk}$). The result of interaction of the parties is always only common secret denoted by K. We don't consider the case when the goal of AKE protocol is to negotiate some public information between two parties. Such protocols (e.g. full-fledged SIGMA-R protocol from [20]) are described in this paper for the case when there is no public information to negotiate.

Verification procedures are described in abbreviated form. Verification of signatures and message authentication codes is simply denoted by «Verify σ, τ», omitting those calculations that are necessary for this, except for the calculation of keys. For example, in the protocol SIGMA-opt1 described in Section 5.48, «Verify σ_A» hides the precomputation of the $\mathsf{MAC}_{K^a}(A)$ value. If a condition is specified after the word «Verify», it means that this condition is to be checked. Also we do not indicate that if the verification failed, the party terminates the protocol execution and returns an error.

We try to ensure that private keys are used either only in group computations, or only in one specific cryptographic primitive such as a signature or a public key encryption scheme. In cases when the authors of the protocol allow such a possibility, we split the keys in the way specified above (e.g. protocol with splitted keys is described in Section 5.89).

In cases when a party checks some ratio, which includes some values received from the channel and some other values which are already known to the party, and designations for these values coincide, we add an overline to the received values («Verify $\overline{B} = B$»).

When describing a message, we always specify identifiers of the parties first if they are included in this message. If the same identifiers are forwarded through the channel several times, then for brevity we do not indicate these repeated transfers.

4 Chronology

The table below lists the protocols in the chronological order. For each protocol we specify the paper in which the protocol was introduced and a number of section with its description. Symbol «*» denotes that the protocol name is not the original name proposed by the authors and is firstly appeared in this paper. Symbol «°» denotes that the protocol is initially introduced as a «toy-protocol» for educational and methodological purposes.

Year	Name	Paper	Section
1976	DH	[1]	5.1
1986	MTI/A0	[2]	5.2
1986	MTI/B0	[2]	5.3
1986	MTI/C0	[2]	5.4
1992	STS-ENC	[3]	5.5
1992	STS-Toy1°	[3]	5.6
1992	STS-Toy2°	[3]	5.7
1992	STS-Toy3°	[3]	5.8
1992	STS-Toy4°	[3]	5.9
1992	STS-MAC	[3]	5.10
1993	ISO93-KE*	[4]	5.11
1994	NR	[5, 9]	5.12
1995	MQV-P1*	[6]	5.13
1995	mMQV-P1*	[6]	5.14
1995	MQV-P2*	[6]	5.15
1995	MQV-P3*	[6]	5.16
1995	mMQV-P3*	[6]	5.17
1995	mMTI/A0*	[6]	5.18
1995	mMTI/B0*	[6]	5.19
1995	mMTI/C0*	[6]	5.20
1995	mNR*	[6]	5.21
1996	mSTS*	[8]	5.22
1997	B-WJM1*	[10]	5.23
1997	B-WJM2*	[10]	5.24
1997	B-WJM3*	[10]	5.25
1997	B-WJM4*	[10]	5.26
1998	KEA	[12]	5.27
1998	LMQSV-P1*	[13, 21]	5.28
1998	LMQSV-P2*	[13, 21]	5.29
1998	LMQSV-P3*	[13, 21]	5.30
1998	LLK	[14]	5.31
2000	SK4*	[17]	5.32
2000	SK4-i*	[17]	5.33
2000	SK4-ii*	[17]	5.34
2000	SK5*	[17]	5.35
2000	SK6*	[17]	5.36
2001	SIG-DH	[18]	5.37
2001	ENC	[18]	5.38
2001	REKEY-AM	[18]	5.39
2001	REKEY-UM	[18]	5.40
2003	Toy1*°	[20]	5.41
2003	Toy2*°	[20]	5.42
2003	BADH°	[20]	5.43
2003	ISO93-KE-4m*	[20]	5.44
2003	ISO93-KE-ab*	[20]	5.45
2003	SIGMA	[20]	5.46
2003	SIGMA-toy*°	[20]	5.47
2003	SIGMA-opt1*	[20]	5.48
2003	SIGMA-opt2*	[20]	5.49
2003	SIGMA-I	[20]	5.50
2003	SIGMA-I-opt1*	[20]	5.51
2003	SIGMA-I-opt2*	[20]	5.52
2003	sSIGMA-R*°	[20]	5.53
2003	sSIGMA-R1*	[20]	5.54
2003	sSIGMA-R2*	[20]	5.55
2003	sSIGMA-R3*	[20]	5.56
2003	SIGMA-R	[20]	5.57
2003	SIGMA-R-opt1*	[20]	5.58
2003	SIGMA-R-opt2*	[20]	5.59
2003	SSEB*	[23]	5.60
2003	SSEB+C*	[23]	5.61
2004	P*	[24]	5.62
2004	TS3	[26, 27]	5.63
2004	TS3-1*	[26, 27]	5.64
2005	HMQV	[28]	5.65

2005	HMQV-C	[28]	5.66
2005	HMQV-1P	[28]	5.67
2005	KEA+	[29]	5.68
2005	KEA+C	[29]	5.69
2005	ECKE-1	[58]	5.70
2006	NAXOS	[31]	5.71
2006	KAM	[32]	5.72
2007	CMQV-2*	[33, 38]	5.73
2007	CMQV-1*	[33, 38]	5.74
2007	ECKE-1N	[34]	5.75
2008	TS1	[26, 27]	5.76
2008	TS2	[26, 27]	5.77
2008	HC*	[35]	5.78
2008	NAXOS+	[36]	5.79
2008	NAXOS+1p*	[36]	5.80
2008	NAXOS+C	[36]	5.81
2009	FHMQV	[37]	5.82
2009	FHMQV-C	[37]	5.83
2009	SIG-DH+	[39]	5.84
2010	SMQV	[40]	5.85
2010	YAK	[41]	5.86
2010	EECKE-1N	[42]	5.87
2011	TMQV	[43]	5.88
2011	CF	[44]	5.89
2012	CMQV+	[45]	5.90
2012	GC	[46]	5.91
2015	sHMQV	[48]	5.92
2017	Echinacea-3	[51]	5.93
2017	Echinacea-3-psk*	[51]	5.94
2017	Echinacea-2	[51]	5.95
2017	Echinacea-2-psk*	[51]	5.96
2017	Limonnik-3	[51]	5.97
2017	Limonnik-3-psk*	[51]	5.98
2017	eFHMQV	[52]	5.99
2019	$\mathcal{C}_{\mathsf{SigMA}}$	[53]	5.100

5 Protocols

5.1 DH

A		**B**
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, E_B}$	$E_B \leftarrow e_B \cdot P$
$K \leftarrow e_A \cdot E_B$		$K \leftarrow e_B \cdot E_A$
return K		**return** K

5.2 MTI/A0

A : x_A, X_A		**B** : x_B, X_B
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, E_B}$	$E_B \leftarrow e_B \cdot P$
$K \leftarrow x_A \cdot E_B + e_A \cdot X_B$		$K \leftarrow e_B \cdot X_A + x_B \cdot E_A$
return K		**return** K

5.3 MTI/B0

A : x_A, X_A		**B** : x_B, X_B
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$Z_A \leftarrow e_A \cdot X_B$	$\xrightarrow{A, Z_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, Z_B}$	$Z_B \leftarrow e_B \cdot X_A$
$K \leftarrow 1/x_A \cdot Z_B + e_A \cdot P$		$K \leftarrow 1/x_B \cdot Z_A + e_B \cdot P$
return K		**return** K

5.4 MTI/C0

$\mathbf{A}: x_A, X_A$		$\mathbf{B}: x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$Z_A \leftarrow e_A \cdot X_B$	$\xrightarrow{A, Z_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, Z_B}$	$Z_B \leftarrow e_B \cdot X_A$
$K \leftarrow 1/x_A \cdot e_A \cdot Z_B$		$K \leftarrow 1/x_B \cdot e_B \cdot Z_A$
return K		**return** K

5.5 STS-ENC

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_B, E_A)$
		$K \leftarrow e_B \cdot E_A$
$K \leftarrow e_A \cdot E_B$	$\xleftarrow{B, E_B, r_B}$	$r_B \leftarrow \mathcal{SE}.\mathsf{Enc}_K(\sigma_B)$
$\sigma_B \leftarrow \mathcal{SE}.\mathsf{Dec}_K(r_B)$		
Verify σ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_A, E_B)$		
$r_A \leftarrow \mathcal{SE}.\mathsf{Enc}_K(\sigma_A)$	$\xrightarrow{A, r_A}$	$\sigma_A \leftarrow \mathcal{SE}.\mathsf{Dec}_K(r_A)$
		Verify σ_A
return K		**return** K

5.6 STS-Toy1

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
Verify σ_B	$\xleftarrow{B, E_B, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_B, E_A)$
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_A, E_B)$	$\xrightarrow{A, \sigma_A}$	Verify σ_A
$K \leftarrow e_A \cdot E_B$		$K \leftarrow e_B \cdot E_A$
return K		**return** K

5.7 STS-Toy2

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_B)$
		$K \leftarrow e_B \cdot E_A$
$K \leftarrow e_A \cdot E_B$	$\xleftarrow{B, E_B, r_B}$	$r_B \leftarrow \mathcal{SE}.\mathsf{Enc}_K(\sigma_B)$
$\sigma_B \leftarrow \mathcal{SE}.\mathsf{Dec}_K(r_B)$		
Verify σ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_A)$		
$r_A \leftarrow \mathcal{SE}.\mathsf{Enc}_K(\sigma_A)$	$\xrightarrow{A, r_A}$	$\sigma_A \leftarrow \mathcal{SE}.\mathsf{Dec}_K(r_A)$
		Verify σ_A
return K		**return** K

5.8 STS-Toy3

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A)$
		$K \leftarrow e_B \cdot E_A$
$K \leftarrow e_A \cdot E_B$	$\xleftarrow{B, E_B, r_B}$	$r_B \leftarrow \mathcal{SE}.\mathsf{Enc}_K(\sigma_B)$
$\sigma_B \leftarrow \mathcal{SE}.\mathsf{Dec}_K(r_B)$		
Verify σ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B)$		
$r_A \leftarrow \mathcal{SE}.\mathsf{Enc}_K(\sigma_A)$	$\xrightarrow{A, r_A}$	$\sigma_A \leftarrow \mathcal{SE}.\mathsf{Dec}_K(r_A)$
		Verify σ_A
return K		**return** K

5.9 STS-Toy4

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(\mathsf{c}_1)$
		$K \leftarrow e_B \cdot E_A$
$K \leftarrow e_A \cdot E_B$	$\xleftarrow{B, E_B, r_B}$	$r_B \leftarrow \mathcal{SE}.\mathsf{Enc}_K(\sigma_B)$
$\sigma_B \leftarrow \mathcal{SE}.\mathsf{Dec}_K(r_B)$		
Verify σ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(\mathsf{c}_2)$		
$r_A \leftarrow \mathcal{SE}.\mathsf{Enc}_K(\sigma_A)$	$\xrightarrow{A, r_A}$	$\sigma_A \leftarrow \mathcal{SE}.\mathsf{Dec}_K(r_A)$
		Verify σ_A
return K		**return** K

5.10 STS-MAC

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_B, E_A)$
		$K \leftarrow e_B \cdot E_A$
$K \leftarrow e_A \cdot E_B$	$\xleftarrow{B, E_B, \sigma_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_K(\sigma_B)$
Verify σ_B, τ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_A, E_B)$		
$\tau_A \leftarrow \mathsf{MAC}_K(\sigma_A)$	$\xrightarrow{A, \sigma_A, \tau_A}$	Verify σ_A, τ_A
return K		**return** K

5.11 ISO93-KE

The description is taken from [20]. This is also the upper-left "toy" protocol in Figure 1 in [20].

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
Verify σ_B	$\xleftarrow{B, E_B, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B, A)$
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B, E_A, B)$	$\xrightarrow{\sigma_A}$	Verify σ_A
$K \leftarrow \mathsf{KDF}(e_A \cdot E_B)$		$K \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
return K		**return** K

5.12 NR

We describe the generalized protocol introduced in [9], any particular variant of the protocol is defined by the choice of coefficients a, b, c.

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$r, u \xleftarrow{U} \mathbb{Z}_q^*$		
$W \leftarrow u \cdot X_B - r \cdot P$		
compute s :		
$ar + b \cdot x_A + c = 0$	$\xrightarrow{A, W, s}$	$R \leftarrow -1/a \cdot (c \cdot P + b \cdot X_A)$
$K \leftarrow u \cdot P$		$K \leftarrow 1/x_B \cdot (W + R)$
return K		**return** K

where (a, b, c) is a permutation of $(\pm\mu(W), \pm s, \pm 1)$.

5.13 MQV-P1

This protocol is called Protocol 1 in the original paper [6].

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$		
$s_A \leftarrow e_A - x_A \cdot \mu(E_A)$	$\xrightarrow{A, E_A, s_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
	$\xleftarrow{B, E_B, s_B}$	$s_B \leftarrow e_B - x_B \cdot \mu(E_B)$
Verify $s_B \cdot P + \mu(E_B) \cdot X_B = E_B$		Verify $s_A \cdot P + \mu(E_A) \cdot X_A = E_A$
$K \leftarrow e_A \cdot E_B$		$K \leftarrow e_B \cdot E_A$
return K		**return** K

5.14 mMQV-P1

This protocol is a modification of Protocol 1 from the paper [6].

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$		
$e'_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E'_A \leftarrow e'_A \cdot P$		
$s_A \leftarrow e_A - x_A \cdot \mu(E_A)$	$\xrightarrow{A, E_A, E'_A, s_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$e'_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E'_B \leftarrow e'_B \cdot P$
	$\xleftarrow{B, E_B, E'_B, s_B}$	$s_B \leftarrow e_B - x_B \cdot \mu(E_B)$
Verify $s_B \cdot P + \mu(E_B) \cdot X_B = E_B$		Verify $s_A \cdot P + \mu(E_A) \cdot X_A = E_A$
$K \leftarrow \nu(e_A \cdot E_B) \oplus \nu(e'_A \cdot E'_B)$		$K \leftarrow \nu(e_B \cdot E_A) \oplus \nu(e'_B \cdot E'_A)$
return K		**return** K

5.15 MQV-P2

This protocol is called Protocol 2 in the original paper [6].

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$Z_A \leftarrow e_A \cdot X_B$		
$E_A \leftarrow e_A \cdot P$		
$s_A \leftarrow e_A + x_A \cdot \mu(Z_A)$	$\xrightarrow{A, E_A, s_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$Z_B \leftarrow e_B \cdot X_A$
		$E_B \leftarrow e_B \cdot P$
	$\xleftarrow{B, E_B, s_B}$	$s_B \leftarrow e_B + x_B \cdot \mu(Z_B)$
$Z_B \leftarrow x_A \cdot E_B$		$Z_A \leftarrow x_B \cdot E_A$
Verify $s_B \cdot P - \mu(Z_B) \cdot X_B = E_B$		Verify $s_A \cdot P - \mu(Z_A) \cdot X_A = E_A$
$K \leftarrow Z_B + Z_A$		$K \leftarrow Z_A + Z_B$
return K		**return** K

5.16 MQV-P3

This protocol is called Protocol 3 in the original paper [6].

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$		
$s_A \leftarrow e_A - x_A \cdot \mu(E_A)$	$\xrightarrow{A, E_A, s_A}$	Verify $s_A \cdot P + \mu(E_A) \cdot X_A = E_A$
$K \leftarrow e_A \cdot X_B$		$K \leftarrow x_B \cdot E_A$
return K		**return** K

5.17 mMQV-P3

This protocol is a modification of Protocol 3 from the paper [6].

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$rnd \in \{0,1\}^\lambda$	$\xrightarrow{A, rnd}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
Verify $s_B \cdot P + \mu(E_B) \cdot X_B = E_B$	$\xleftarrow{B, E_B, s_B}$	$s_B \leftarrow e_B - x_B \cdot \mu(E_B)$
$K \leftarrow \nu(x_A \cdot E_B) \oplus rnd$		$K \leftarrow \nu(e_B \cdot X_A) \oplus rnd$
return K		**return** K

5.18 mMTI/A0

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K \leftarrow e_B \cdot X_A + x_B \cdot E_A$
$K \leftarrow x_A \cdot E_B + e_A \cdot X_B$	$\xleftarrow{B, E_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_K(E_B)$
Verify τ_B		
return K		**return** K

5.19 mMTI/B0

$\mathbf{A}: x_A, X_A$		$\mathbf{B}: x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$Z_A \leftarrow e_A \cdot X_B$	$\xrightarrow{A, Z_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$Z_B \leftarrow e_B \cdot X_A$
		$K \leftarrow 1/x_B \cdot Z_A + e_B \cdot P$
$K \leftarrow 1/x_A \cdot Z_B + e_A \cdot P$	$\xleftarrow{B, Z_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_K(Z_B)$
Verify τ_B		
return K		**return** K

5.20 mMTI/C0

$\mathbf{A}: x_A, X_A$		$\mathbf{B}: x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$Z_A \leftarrow e_A \cdot X_B$	$\xrightarrow{A, Z_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$Z_B \leftarrow e_B \cdot X_A$
		$K \leftarrow 1/x_B \cdot e_B \cdot Z_A$
$K \leftarrow 1/x_A \cdot e_A \cdot Z_B$	$\xleftarrow{B, Z_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_K(Z_B)$
Verify τ_B		
return K		**return** K

5.21 mNR

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$k \xleftarrow{U} \mathbb{Z}_q^*$		
$r \xleftarrow{U} \mathbb{Z}_q^*$		
$W \leftarrow k \cdot X_B - r \cdot P$		
$s \leftarrow r - \mu(W) \cdot x_A$		
$K \leftarrow k \cdot P$		
$\tau_A \leftarrow \mathsf{MAC}_K(X_A)$	$\xrightarrow{A, W, s, \tau_A}$	$R \leftarrow s \cdot P + \mu(W) \cdot X_A$
		$K \leftarrow 1/x_B \cdot (W + R)$
		Verify τ_A
return K		**return** K

5.22 mSTS

This is the modification of STS protocol described in [8].

$\mathbf{A} : sk_A^s, pk_A^s$		$\mathbf{B} : sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K \leftarrow e_B \cdot E_A$
$K \leftarrow e_A \cdot E_B$	$\xleftarrow{B, E_B, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B, \mathsf{H}(K))$
Verify σ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B, E_A, \mathsf{H}(K))$	$\xrightarrow{A, \sigma_A}$	Verify σ_A
return K		**return** K

5.23 B-WJM1

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K^a \leftarrow \mathsf{KDF}(x_B \cdot X_A, \mathsf{c}_1)$
$K^a \leftarrow \mathsf{KDF}(x_A \cdot X_B, \mathsf{c}_1)$	$\xleftarrow{B, E_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_2, B, A, E_B, E_A)$
Verify τ_B		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_3, A, B, E_A, E_B)$	$\xrightarrow{\tau_A}$	Verify τ_A
$K \leftarrow \mathsf{KDF}(e_A \cdot E_B, \mathsf{c}_4)$		$K \leftarrow \mathsf{KDF}(e_B \cdot E_A, \mathsf{c}_4)$
return K		**return** K

5.24 B-WJM2

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A, x_B \cdot X_A)$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot E_B, x_A \cdot X_B)$	$\xleftarrow{B, E_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_1, B, A, E_B, E_A)$
Verify τ_B		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_2, A, B, E_A, E_B)$	$\xrightarrow{\tau_A}$	Verify τ_A
return K		**return** K

5.25 B-WJM3

$\mathbf{A}: x_A, X_A$		$\mathbf{B}: x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, E_B}$	$E_B \leftarrow e_B \cdot P$
$K \leftarrow \mathsf{KDF}(e_A \cdot E_B, x_A \cdot X_B)$		$K \leftarrow \mathsf{KDF}(e_B \cdot E_A, x_B \cdot X_A)$
return K		**return** K

5.26 B-WJM4

$\mathbf{A}: x_A, X_A$		$\mathbf{B}: x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, E_B}$	$E_B \leftarrow e_B \cdot P$
$K \leftarrow \mathsf{KDF}(x_A \cdot E_B, e_A \cdot X_B)$		$K \leftarrow \mathsf{KDF}(e_B \cdot X_A, x_B \cdot E_A)$
return K		**return** K

5.27 KEA

$\mathbf{A}: x_A, X_A$		$\mathbf{B}: x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, E_B}$	$E_B \leftarrow e_B \cdot P$
$K \leftarrow \mathsf{KDF}(x_A \cdot E_B + e_A \cdot X_B)$		$K \leftarrow \mathsf{KDF}(e_B \cdot X_A + x_B \cdot E_A)$
return K		**return** K

5.28 LMQSV-P1

This protocol is called Protocol 1 in the original papers [13, 21]. In the subsequent it is usually referred to as MQV protocol (see e.g. [28, 55]).

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, E_B}$	$E_B \leftarrow e_B \cdot P$
$s_A \leftarrow e_A + x_A \cdot \mu(E_A)$		$s_B \leftarrow e_B + x_B \cdot \mu(E_B)$
$K \leftarrow s_A \cdot (E_B + \mu(E_B) \cdot X_B)$		$K \leftarrow s_B \cdot (E_A + \mu(E_A) \cdot X_A)$
return K		**return** K

5.29 LMQSV-P2

This protocol is called Protocol 2 in the original papers [13, 21].

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	
$s_A \leftarrow e_A + x_A \cdot \mu(E_A)$		$s_B \leftarrow x_B + x_B \cdot \mu(X_B)$
$K \leftarrow s_A \cdot (X_B + \mu(X_B) \cdot X_B)$		$K \leftarrow s_B \cdot (E_A + \mu(E_A) \cdot X_A)$
return K		**return** K

5.30 LMQSV-P3

This protocol is called Protocol 3 in the original papers [13, 21].

$\mathbf{A}: x_A, X_A$		$\mathbf{B}: x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$s_B \leftarrow e_B + x_B \cdot \mu(E_B)$
		$Q \leftarrow s_B \cdot (E_A + \mu(E_A) \cdot X_A)$
		$K, K^a \leftarrow \mathsf{KDF}(Q)$
$s_A \leftarrow e_A + x_A \cdot \mu(E_A)$	$\xleftarrow{B, E_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_1, B, A, E_B, E_A)$
$Q \leftarrow s_A \cdot (E_B + \mu(E_B) \cdot X_B)$		
$K, K^a \leftarrow \mathsf{KDF}(Q)$		
Verify τ_B		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_2, A, B, E_A, E_B)$	$\xrightarrow{\tau_A}$	Verify τ_A
return K		**return** K

5.31 LLK

$\mathbf{A}: x_A, X_A$		$\mathbf{B}: x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$Z_A \leftarrow e_A \cdot X_B$	$\xrightarrow{A, Z_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$K \leftarrow Z_A + e_B \cdot X_A$
$K \leftarrow Z_A + (x_A/(x_A + e_A)) \cdot W_B$	$\xleftarrow{B, W_B}$	$W_B \leftarrow e_B \cdot X_A + (e_B/x_B) \cdot Z_A$
return K		**return** K

5.32 SK4

This protocol is called Protocol 4 in the original paper [17].

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, E_B}$	$E_B \leftarrow e_B \cdot P$
$K \leftarrow \mathsf{KDF}(e_A \cdot X_B + (x_A + e_A) \cdot E_B)$		$K \leftarrow \mathsf{KDF}(e_B \cdot X_A + (x_B + e_B) \cdot E_A)$
return K		**return** K

5.33 SK4-i

This is Protocol 4 from [17] with a session key calculated according to variation i.

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, E_B}$	$E_B \leftarrow e_B \cdot P$
$K \leftarrow \mathsf{KDF}(e_A \cdot X_B + x_A \cdot E_B, e_A \cdot E_B)$		$K \leftarrow \mathsf{KDF}(e_B \cdot X_A + x_B \cdot E_A, e_B \cdot E_A)$
return K		**return** K

5.34 SK4-ii

This is Protocol 4 from [17] with a session key calculated according to variation ii.

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, E_B}$	$E_B \leftarrow e_B \cdot P$
$K \leftarrow \mathsf{KDF}(e_A \cdot X_B, x_A \cdot E_B, e_A \cdot E_B)$		$K \leftarrow \mathsf{KDF}(x_B \cdot E_A, e_B \cdot X_A, e_B \cdot E_A)$
return K		**return** K

5.35 SK5

This protocol is called Protocol 5 in the original paper [17].

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot X_A + (x_B + e_B) \cdot E_A)$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot X_B + (x_A + e_A) \cdot E_B)$	$\xleftarrow{B, E_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_1, B, A, E_B, E_A)$
Verify τ_B		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_2, A, B, E_A, E_B)$	$\xrightarrow{\tau_A}$	Verify τ_A
return K		**return** K

5.36 SK6

This protocol is called Protocol 6 in the original paper [17].

$\mathbf{A} : (x_A, X_A), (sk_A^s, pk_A^s)$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_A, A)$	$\xrightarrow{A, E_A, \sigma_A}$	Verify σ_A
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot X_A + (x_B + e_B) \cdot E_A)$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot X_B + (x_A + e_A) \cdot E_B)$	$\xleftarrow{B, E_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(B, A, E_B, E_A)$
Verify τ_B		
return K		**return** K

5.37 SIG-DH

$\mathbf{A} : (sk_A^s, pk_A^s), \mathsf{sid}$		$\mathbf{B} : (sk_B^s, pk_B^s), \mathsf{sid}$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, \mathsf{sid}, E_A}$	Verify $\overline{\mathsf{sid}} = \mathsf{sid}$
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
Verify σ_B	$\xleftarrow{B, E_B, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(B, \mathsf{sid}, E_B, E_A, A)$
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(A, \mathsf{sid}, E_A, E_B, B)$	$\xrightarrow{\sigma_A}$	Verify σ_A
$K \leftarrow e_A \cdot E_B$		$K \leftarrow e_B \cdot E_A$
return K		**return** K

5.38 ENC

$\mathbf{A}$: sid		$\mathbf{B}$: (sk_B^e, pk_B^e), sid
$K^* \xleftarrow{U} \{0,1\}^\lambda$		
$C_A \leftarrow \mathcal{PKE}.\mathsf{Enc}_{pk_B^e}(K^*)$	$\xrightarrow{A, \mathsf{sid}, C_A}$	Verify $\overline{\mathsf{sid}} = \mathsf{sid}$
		$K^* \leftarrow \mathcal{PKE}.\mathsf{Dec}_{sk_B^e}(C_A)$
$K \leftarrow \mathsf{KDF}(K^*, A, B, \mathsf{sid})$		$K \leftarrow \mathsf{KDF}(K^*, A, B, \mathsf{sid})$
return K		**return** K

5.39 REKEY-AM

$\mathbf{A}$: psk, sid		$\mathbf{B}$: psk, sid
$r_A \xleftarrow{U} \{0,1\}^{2\lambda}$	$\xrightarrow{A, \mathsf{sid}, r_A}$	Verify $\overline{\mathsf{sid}} = \mathsf{sid}$
	$\xleftarrow{B, r_B}$	$r_B \xleftarrow{U} \{0,1\}^{2\lambda}$
$K \leftarrow \mathsf{KDF}(\mathsf{psk}, r_A, r_B)$		$K \leftarrow \mathsf{KDF}(\mathsf{psk}, r_A, r_B)$
return K		**return** K

5.40 REKEY-UM

$\mathbf{A}$: psk, sid		$\mathbf{B}$: psk, sid
$r_A \xleftarrow{U} \{0,1\}^{2\lambda}$	$\xrightarrow{A, \mathsf{sid}, r_A}$	Verify $\overline{\mathsf{sid}} = \mathsf{sid}$
		$r_B \xleftarrow{U} \{0,1\}^{2\lambda}$
$K^a, K^* \leftarrow \mathsf{KDF}(\mathsf{psk})$		$K^a, K^* \leftarrow \mathsf{KDF}(\mathsf{psk})$
Verify τ_B	$\xleftarrow{B, r_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(A, r_A, \mathsf{sid}, r_B)$
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(B, r_B, \mathsf{sid}, r_A)$	$\xrightarrow{\tau_A}$	Verify τ_A
$K \leftarrow \mathsf{KDF}(K^*, r_A, r_B)$		$K \leftarrow \mathsf{KDF}(K^*, r_A, r_B)$
return K		**return** K

5.41 Toy1

This is the upper-right protocol in Figure 1 in [20].

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
Verify σ_B	$\xleftarrow{B, E_B, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B, B)$
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B, E_A, A)$	$\xrightarrow{\sigma_A}$	Verify σ_A
$K \leftarrow \mathsf{KDF}(e_A \cdot E_B)$		$K \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
return K		**return** K

5.42 Toy2

This is the lower-right protocol in Figure 1 in [20].

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B, B)$
		$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{B, E_B, \sigma_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\sigma_B)$
Verify σ_B, τ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B, E_A, A)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\sigma_A)$	$\xrightarrow{\sigma_A, \tau_A}$	Verify σ_A, τ_A
return K		**return** K

5.43 BADH

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
Verify σ_B	$\xleftarrow{B, E_B, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B)$
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B, E_A)$	$\xrightarrow{A, \sigma_A}$	Verify σ_A
$K \leftarrow \mathsf{KDF}(e_A \cdot E_B)$		$K \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
return K		**return** K

5.44 ISO93-KE-4m

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$K, K^e \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
		$C_B \leftarrow \mathcal{SE}.\mathsf{Enc}_{K^e}(B)$
$K, K^e \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{E_B, C_B}$	$E_B \leftarrow e_B \cdot P$
$B \leftarrow \mathcal{SE}.\mathsf{Dec}_{K^e}(C_B)$		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B, E_A, B)$		
$C_A \leftarrow \mathcal{SE}.\mathsf{Enc}_{K^e}(A, \sigma_A)$	$\xrightarrow{C_A}$	$A, \sigma_A \leftarrow \mathcal{SE}.\mathsf{Dec}_{K^e}(C_A)$
		Verify σ_A
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B, A)$
$\sigma_B \leftarrow \mathcal{SE}.\mathsf{Dec}_{K^e}(C'_B)$	$\xleftarrow{C'_B}$	$C'_B \leftarrow \mathcal{SE}.\mathsf{Enc}_{K^e}(\sigma_B)$
Verify σ_B		
return K		**return** K

5.45 ISO93-KE-ab

This protocol is described in [20] only at the idea level («We only sketch the idea behind this protocol») and called «alias-based», so we call it here with suffix «-ab».

$\mathbf{A} : sk_A^s, pk_A^s$		$\mathbf{B} : sk_B^s, pk_B^s$
$r \xleftarrow{U} \{0,1\}^\lambda$		
$\widehat{A} \leftarrow \mathsf{H}(A, r)$		
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{\widehat{A}, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B, \widehat{A})$
		$K, K^e \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
$K, K^e \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{E_B, C_B}$	$C_B \leftarrow \mathcal{SE}.\mathsf{Enc}_{K^e}(B, \sigma_B)$
$B, \sigma_B \leftarrow \mathcal{SE}.\mathsf{Dec}_{K^e}(C_B)$		
Verify σ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B, E_A, B)$		
$C_A \leftarrow \mathcal{SE}.\mathsf{Enc}_{K^e}(A, r, \sigma_A)$	$\xrightarrow{C_A}$	$A, r, \sigma_A \leftarrow \mathcal{SE}.\mathsf{Dec}_{K^e}(C_A)$
		Verify $\widehat{A} = \mathsf{H}(A, r), \sigma_A$
return K		**return** K

5.46 SIGMA

In addition to the SIGMA protocol described in this section, the authors of [20] discuss the possibility of re-using the ephemeral keys in this protocol. This means that ephemeral keys become long-term, and this could be described as a separate protocol, but the description in [20] is so vague that it cannot be done.

$\mathbf{A} : sk_A^s, pk_A^s$		$\mathbf{B} : sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$ $K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$ $\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B)$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{B, E_B, \sigma_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(B)$
Verify σ_B, τ_B $\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B, E_A)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(A)$	$\xrightarrow{A, \sigma_A, \tau_A}$	Verify σ_A, τ_A
return K		**return** K

5.47 SIGMA-toy

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B)$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{B, E_B, \sigma_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(B)$
Verify σ_B, τ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_A, E_B)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(A)$	$\xrightarrow{A, \sigma_A, \tau_A}$	Verify σ_A, τ_A
return K		**return** K

5.48 SIGMA-opt1

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{B, E_B, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B, \mathsf{MAC}_{K^a}(B))$
Verify σ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B, E_A, \mathsf{MAC}_{K^a}(A))$	$\xrightarrow{A, \sigma_A}$	Verify σ_A
return K		**return** K

5.49 SIGMA-opt2

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{B, E_B, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(\mathsf{MAC}_{K^a}(E_A, E_B, B))$
Verify σ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(\mathsf{MAC}_{K^a}(E_B, E_A, A))$	$\xrightarrow{A, \sigma_A}$	Verify σ_A
return K		**return** K

5.50 SIGMA-I

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K, K^a, K^{ae} \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B)$
		$\tau_B \leftarrow \mathsf{MAC}_{K^a}(B)$
$K, K^a, K^{ae} \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{E_B, C_B}$	$C_B \leftarrow \mathcal{AE}.\mathsf{Enc}_{K^{ae}}(\varepsilon, (B, \sigma_B, \tau_B))$
$B, \sigma_B, \tau_B \leftarrow \mathcal{AE}.\mathsf{Dec}_{K^{ae}}(\varepsilon, C_B)$		
Verify σ_B, τ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B, E_A)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(A)$		
$C_A \leftarrow \mathcal{AE}.\mathsf{Enc}_{K^{ae}}(\varepsilon, (A, \sigma_A, \tau_A))$	$\xrightarrow{C_A}$	$A, \sigma_A, \tau_A \leftarrow \mathcal{AE}.\mathsf{Dec}_{K^{ae}}(\varepsilon, C_A)$
		Verify σ_A, τ_A
return K		**return** K

5.51 SIGMA-I-opt1

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K, K^a, K^{ae} \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B, \mathsf{MAC}_{K^a}(B))$
$K, K^a, K^{ae} \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{E_B, C_B}$	$C_B \leftarrow \mathcal{AE}.\mathsf{Enc}_{K^{ae}}(\varepsilon, (B, \sigma_B))$
$B, \sigma_B \leftarrow \mathcal{AE}.\mathsf{Dec}_{K^{ae}}(\varepsilon, C_B)$		
Verify σ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B, E_A, \mathsf{MAC}_{K^a}(A))$		
$C_A \leftarrow \mathcal{AE}.\mathsf{Enc}_{K^{ae}}(\varepsilon, (A, \sigma_A))$	$\xrightarrow{C_A}$	$A, \sigma_A \leftarrow \mathcal{AE}.\mathsf{Dec}_{K^{ae}}(\varepsilon, C_A)$
		Verify σ_A
return K		**return** K

5.52 SIGMA-I-opt2

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K, K^a, K^{ae} \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(\mathsf{MAC}_{K^a}(E_A, E_B, B))$
$K, K^a, K^{ae} \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{E_B, C_B}$	$C_B \leftarrow \mathcal{AE}.\mathsf{Enc}_{K^{ae}}(\varepsilon, (B, \sigma_B))$
$B, \sigma_B \leftarrow \mathcal{AE}.\mathsf{Dec}_{K^{ae}}(\varepsilon, C_B)$		
Verify σ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(\mathsf{MAC}_{K^a}(E_B, E_A, A))$		
$C_A \leftarrow \mathcal{AE}.\mathsf{Enc}_{K^{ae}}(\varepsilon, (A, \sigma_A))$	$\xrightarrow{C_A}$	$A, \sigma_A \leftarrow \mathcal{AE}.\mathsf{Dec}_{K^{ae}}(\varepsilon, C_A)$
		Verify σ_A
return K		**return** K

5.53 sSIGMA-R

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{E_B}$	$E_B \leftarrow e_B \cdot P$
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(A)$		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B, E_A)$	$\xrightarrow{A, \sigma_A, \tau_A}$	$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
		Verify σ_A, τ_A
		$\tau_B \leftarrow \mathsf{MAC}_{K^a}(B)$
Verify σ_B, τ_B	$\xleftarrow{B, \sigma_B, \tau_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B)$
return K		**return** K

5.54 sSIGMA-R1

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{E_B}$	$E_B \leftarrow e_B \cdot P$
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_1, A)$		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B, E_A)$	$\xrightarrow{A, \sigma_A, \tau_A}$	$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
		Verify σ_A, τ_A
		$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_2, B)$
Verify σ_B, τ_B	$\xleftarrow{B, \sigma_B, \tau_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B)$
return K		**return** K

5.55 sSIGMA-R2

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
$K, K_A^a, K_B^a \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{E_B}$	$E_B \leftarrow e_B \cdot P$
$\tau_A \leftarrow \mathsf{MAC}_{K_A^a}(A)$		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B, E_A)$	$\xrightarrow{A, \sigma_A, \tau_A}$	$K, K_A^a, K_B^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
		Verify σ_A, τ_A
		$\tau_B \leftarrow \mathsf{MAC}_{K_B^a}(B)$
Verify σ_B, τ_B	$\xleftarrow{B, \sigma_B, \tau_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B)$
return K		**return** K

5.56 sSIGMA-R3

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
Verify $E_A \neq E_B$	$\xleftarrow{E_B}$	$E_B \leftarrow e_B \cdot P$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot E_B)$ $\tau_A \leftarrow \mathsf{MAC}_{K^a}(A)$		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_B, E_A)$	$\xrightarrow{A, \sigma_A, \tau_A}$	$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
		Verify σ_A, τ_A $\tau_B \leftarrow \mathsf{MAC}_{K^a}(B)$
Verify σ_B, τ_B	$\xleftarrow{B, \sigma_B, \tau_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B)$
return K		**return** K

5.57 SIGMA-R

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$n_A \xleftarrow{U} \{0,1\}^\lambda$		
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A, n_A}$	$n_B \xleftarrow{U} \{0,1\}^\lambda$
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
$K, K_A^a, K_B^a, K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{E_B, n_B}$	$E_B \leftarrow e_B \cdot P$
$\tau_A \leftarrow \mathsf{MAC}_{K_A^a}(A)$		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(n_B, E_A)$		
$C_A \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_A^{ae}}(\varepsilon, (A, \sigma_A, \tau_A))$	$\xrightarrow{C_A}$	$K, K_A^a, K_B^a, K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
		$A, \sigma_A, \tau_A \leftarrow \mathcal{AE}.\mathsf{Dec}_{K_A^{ae}}(\varepsilon, C_A)$
		Verify σ_A, τ_A
		$\tau_B \leftarrow \mathsf{MAC}_{K_B^a}(B)$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(n_A, E_B)$
$B, \sigma_B, \tau_B \leftarrow \mathcal{AE}.\mathsf{Dec}_{K_B^{ae}}(\varepsilon, C_B)$	$\xleftarrow{C_B}$	$C_B \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_B^{ae}}(\varepsilon, (B, \sigma_B, \tau_B))$
Verify σ_B, τ_B		
return K		**return** K

5.58 SIGMA-R-opt1

$\mathbf{A}$: sk_A^s, pk_A^s		$\mathbf{B}$: sk_B^s, pk_B^s
$n_A \xleftarrow{U} \{0,1\}^\lambda$		
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A, n_A}$	$n_B \xleftarrow{U} \{0,1\}^\lambda$
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
$K, K_A^a, K_B^a, K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{E_B, n_B}$	$E_B \leftarrow e_B \cdot P$
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(n_B, E_A, \mathsf{MAC}_{K_A^a}(A))$		
$C_A \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_A^{ae}}(\varepsilon, (A, \sigma_A))$	$\xrightarrow{C_A}$	$K, K_A^a, K_B^a, K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
		$A, \sigma_A \leftarrow \mathcal{AE}.\mathsf{Dec}_{K_A^{ae}}(\varepsilon, C_A)$
		Verify σ_A
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(n_A, E_B, \mathsf{MAC}_{K_B^a}(B))$
$B, \sigma_B \leftarrow \mathcal{AE}.\mathsf{Dec}_{K_B^{ae}}(\varepsilon, C_B)$	$\xleftarrow{C_B}$	$C_B \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_B^{ae}}(\varepsilon, (B, \sigma_B))$
Verify σ_B		
return K		**return** K

5.59 SIGMA-R-opt2

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$n_A \xleftarrow{U} \{0,1\}^\lambda$		
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{E_A, n_A}$	$n_B \xleftarrow{U} \{0,1\}^\lambda$
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
$K, K_A^a, K_B^a, K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{E_B, n_B}$	$E_B \leftarrow e_B \cdot P$
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(\mathsf{MAC}_{K_A^a}(n_B, E_A, A))$		
$C_A \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_A^{ae}}(\varepsilon, (A, \sigma_A))$	$\xrightarrow{C_A}$	$K, K_A^a, K_B^a, K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
		$A, \sigma_A \leftarrow \mathcal{AE}.\mathsf{Dec}_{K_A^{ae}}(\varepsilon, C_A)$
		Verify σ_A
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(\mathsf{MAC}_{K_B^a}(n_A, E_B, B))$
$B, \sigma_B \leftarrow \mathcal{AE}.\mathsf{Dec}_{K_B^{ae}}(\varepsilon, C_B)$	$\xleftarrow{C_B}$	$C_B \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_B^{ae}}(\varepsilon, (B, \sigma_B))$
Verify σ_B		
return K		**return** K

5.60 SSEB

$\mathbf{A}: x_A, X_A$		$\mathbf{B}: x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$Z_A \leftarrow e_A \cdot X_B$	$\xrightarrow{A, Z_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, Z_B}$	$Z_B \leftarrow e_B \cdot X_A$
$K \leftarrow e_A/x_A \cdot Z_B + x_A \cdot X_B$		$K \leftarrow e_B/x_B \cdot Z_A + x_B \cdot X_A$
return K		**return** K

5.61 SSEB+C

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$Z_A \leftarrow e_A \cdot X_B$	$\xrightarrow{A, Z_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$Z_B \leftarrow e_B \cdot X_A$
		$K, K^a \leftarrow \mathsf{KDF}(e_B / x_B \cdot Z_A + x_B \cdot X_A)$
$K, K^a \leftarrow \mathsf{KDF}(e_A / x_A \cdot Z_B + x_A \cdot X_B)$	$\xleftarrow{B, Z_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_2, B, A, Z_B, Z_A)$
Verify τ_B		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_1, A, B, Z_A, Z_B)$	$\xrightarrow{\tau_A}$	Verify τ_A
return K		**return** K

5.62 P

Here we generalize the original description of the protocol [24] in order to show its cryptographic core. Namely, we consider the result of static Diffie-Hellman as an authentication key and define the usage of MAC function instead of hash function for authentication of ephemeral public values.

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$		
$K^a \leftarrow \mathsf{KDF}(x_A \cdot X_B)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(E_A)$	$\xrightarrow{A, E_A, \tau_A}$	$K^a \leftarrow \mathsf{KDF}(x_B \cdot X_A)$
		Verify τ_A
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_A \cdot P$
Verify τ_B	$\xleftarrow{B, E_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(E_B)$
$K \leftarrow e_A \cdot E_B$		$K \leftarrow e_B \cdot E_A$
return K		**return** K

5.63 TS3

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$		
$K^a \leftarrow \mathsf{KDF}(x_A \cdot X_B)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(A, B, E_A)$	$\xrightarrow{A, E_A, \tau_A}$	$K^a \leftarrow \mathsf{KDF}(x_B \cdot X_A)$
		Verify τ_A
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
Verify τ_B	$\xleftarrow{B, E_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(B, A, E_B)$
$K \leftarrow e_A \cdot E_B$		$K \leftarrow e_B \cdot E_A$
return K		**return** K

5.64 TS3-1

$\mathbf{A} : sk_A^s, pk_A^s$		$\mathbf{B} : sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(A, B, E_A)$	$\xrightarrow{A, E_A, \sigma_A}$	Verify σ_A
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
Verify σ_B	$\xleftarrow{B, E_B, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(B, A, E_B)$
$K \leftarrow e_A \cdot E_B$		$K \leftarrow e_B \cdot E_A$
return K		**return** K

5.65 HMQV

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, E_B}$	$E_B \leftarrow e_B \cdot P$
$d \leftarrow \mathsf{H}(E_A, B)$		$d \leftarrow \mathsf{H}(E_A, B)$
$e \leftarrow \mathsf{H}(E_B, A)$		$e \leftarrow \mathsf{H}(E_B, A)$
$s_A \leftarrow e_A + d \cdot x_A$		$s_B \leftarrow e_B + e \cdot x_B$
$Q \leftarrow s_A \cdot (E_B + e \cdot X_B)$		$Q \leftarrow s_B \cdot (E_A + d \cdot X_A)$
$K \leftarrow \mathsf{KDF}(Q)$		$K \leftarrow \mathsf{KDF}(Q)$
return K		**return** K

5.66 HMQV-C

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, B, E_A}$	Verify $\overline{B} = B$
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$d \leftarrow \mathsf{H}(E_A, B)$
		$e \leftarrow \mathsf{H}(E_B, A)$
		$s_B \leftarrow e_B + e \cdot x_B$
		$Q \leftarrow s_B \cdot (E_A + d \cdot X_A)$
		$K, K^a \leftarrow \mathsf{KDF}(Q)$
$d \leftarrow \mathsf{H}(E_A, B)$	$\xleftarrow{E_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_1)$
$e \leftarrow \mathsf{H}(E_B, A)$		
$s_A \leftarrow e_A + d \cdot x_A$		
$Q \leftarrow s_A \cdot (E_B + e \cdot X_B)$		
$K, K^a \leftarrow \mathsf{KDF}(Q)$		
Verify τ_B		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_2)$	$\xrightarrow{\tau_A}$	Verify τ_A
return K		**return** K

5.67 HMQV-1P

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, B, E_A}$	Verify $\overline{B} = B$
$u \leftarrow \mathsf{H}(E_A, A, B)$		$u \leftarrow \mathsf{H}(E_A, A, B)$
$Q \leftarrow (e_A + u \cdot x_A) \cdot X_B$		$Q \leftarrow x_B \cdot (E_A + u \cdot X_A)$
$K \leftarrow \mathsf{KDF}(Q)$		$K \leftarrow \mathsf{KDF}(Q)$
return K		**return** K

5.68 KEA+

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, E_B}$	$E_B \leftarrow e_B \cdot P$
$K \leftarrow \mathsf{KDF}(x_A \cdot E_B, e_A \cdot X_B, A, B)$		$K \leftarrow \mathsf{KDF}(e_B \cdot X_A, x_B \cdot E_A, A, B)$
return K		**return** K

5.69 KEA+C

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot X_A, x_B \cdot E_A, A, B)$
$K, K^a \leftarrow \mathsf{KDF}(x_A \cdot E_B, e_A \cdot X_B, A, B)$	$\xleftarrow{B, E_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_1)$
Verify τ_B		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_2)$	$\xrightarrow{\tau_A}$	Verify τ_A
return K		**return** K

5.70 ECKE-1

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$s_A \leftarrow \mathsf{H}_1(e_A, x_A, A)$		
$W_A \leftarrow (e_A + s_A \cdot x_A) \cdot P$	$\xrightarrow{A, W_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$s_B \leftarrow \mathsf{H}_1(e_B, x_B, B)$
	$\xleftarrow{B, W_B}$	$W_B \leftarrow (e_B + s_B \cdot x_B) \cdot P$
$r_A \leftarrow x_A \cdot \mathsf{H}_2(W_A, W_B, A, B)$		$r_B \leftarrow x_B \cdot \mathsf{H}_2(W_A, W_B, A, B)$
$K \leftarrow \mathsf{KDF}((e_A + s_A \cdot x_A) \cdot W_B + r_A \cdot X_B)$		$K \leftarrow \mathsf{KDF}((e_B + s_B \cdot x_B) \cdot W_A + r_B \cdot X_A)$
return K		**return** K

5.71 NAXOS

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \{0,1\}^\lambda$		
$W_A \leftarrow \mathsf{H}(e_A, x_A) \cdot P$	$\xrightarrow{A, W_A}$	$e_B \xleftarrow{U} \{0,1\}^\lambda$
	$\xleftarrow{B, W_B}$	$W_B \leftarrow \mathsf{H}(e_B, x_B) \cdot P$
$Q_1 \leftarrow x_A \cdot W_B$		$Q_1 \leftarrow \mathsf{H}(e_B, x_B) \cdot X_A$
$Q_2 \leftarrow \mathsf{H}(e_A, x_A) \cdot X_B$		$Q_2 \leftarrow x_B \cdot W_A$
$Q_3 \leftarrow \mathsf{H}(e_A, x_A) \cdot W_B$		$Q_3 \leftarrow \mathsf{H}(e_B, x_B) \cdot W_A$
$K \leftarrow \mathsf{KDF}(Q_1, Q_2, Q_3, A, B)$		$K \leftarrow \mathsf{KDF}(Q_1, Q_2, Q_3, A, B)$
return K		**return** K

5.72 KAM

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, E_B}$	$E_B \leftarrow e_B \cdot P$
$K_1^a \leftarrow \mathsf{KDF}(x_A \cdot E_B)$		$K_1^a \leftarrow \mathsf{KDF}(e_B \cdot X_A)$
$\tau_A \leftarrow \mathsf{MAC}_{K_1^a}(A, B, E_A)$	$\xrightarrow{\tau_A}$	Verify τ_A
$K_2^a \leftarrow \mathsf{KDF}(e_A \cdot X_B)$		$K_2^a \leftarrow \mathsf{KDF}(x_B \cdot E_A)$
Verify τ_B	$\xleftarrow{\tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K_2^a}(B, A, E_B)$
$K \leftarrow \mathsf{H}(x_A \cdot X_B) \oplus \mathsf{H}(e_A \cdot E_B)$		$K \leftarrow \mathsf{H}(x_B \cdot X_A) \oplus \mathsf{H}(e_B \cdot E_A)$
return K		**return** K

5.73 CMQV-2

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$W_A \leftarrow \mathsf{H}_1(e_A, x_A) \cdot P$	$\xrightarrow{B, A, W_A}$	Verify $\overline{B} = B$
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{W_B}$	$W_B \leftarrow \mathsf{H}_1(e_B, x_B) \cdot P$
$d \leftarrow \mathsf{H}_2(W_A, A, B)$		$d \leftarrow \mathsf{H}_2(W_A, A, B)$
$e \leftarrow \mathsf{H}_2(W_B, A, B)$		$e \leftarrow \mathsf{H}_2(W_B, A, B)$
$t_A \leftarrow \mathsf{H}_1(e_A, x_A) + d \cdot x_A$		$t_B \leftarrow \mathsf{H}_1(e_B, x_B) + e \cdot x_B$
$Q \leftarrow t_A \cdot (W_B + e \cdot X_B)$		$Q \leftarrow t_B \cdot (W_A + d \cdot X_A)$
$K \leftarrow \mathsf{KDF}(Q, W_A, W_B, A, B)$		$K \leftarrow \mathsf{KDF}(Q, W_A, W_B, A, B)$
return K		**return** K

5.74 CMQV-1

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$W_A \leftarrow \mathsf{H}_1(e_A, x_A) \cdot P$	$\xrightarrow{B, A, W_A}$	Verify $\overline{B} = B$
$d \leftarrow \mathsf{H}_2(W_A, A, B)$		$d \leftarrow \mathsf{H}_2(W_A, A, B)$
$Q \leftarrow (\mathsf{H}_1(e_A, x_A) + d \cdot x_A) \cdot X_B$		$Q \leftarrow x_B \cdot (W_A + d \cdot X_A)$
$K \leftarrow \mathsf{KDF}(Q, W_A, A, B)$		$K \leftarrow \mathsf{KDF}(Q, W_A, A, B)$
return K		**return** K

5.75 ECKE-1N

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$Z_A \leftarrow e_A \cdot X_B$	$\xrightarrow{A, Z_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, Z_B}$	$Z_B \leftarrow e_B \cdot X_A$
$w_1 \leftarrow \mathsf{H}(Z_A, B, A)$		$w_1 \leftarrow \mathsf{H}(Z_A, B, A)$
$w_2 \leftarrow \mathsf{H}(Z_B, A, B)$		$w_2 \leftarrow \mathsf{H}(Z_B, A, B)$
$Q \leftarrow x_A^{-1} \cdot (e_A + w_1)(Z_B + w_2 \cdot X_A)$		$Q \leftarrow x_B^{-1} \cdot (e_B + w_2)(Z_A + w_1 \cdot X_B)$
$K \leftarrow \mathsf{KDF}(Q)$		$K \leftarrow \mathsf{KDF}(Q)$
return K		**return** K

5.76 TS1

The original version of this protocol [26] does not assume including parties identifiers in the KDF function arguments during the session key computation ($K \leftarrow \mathsf{KDF}(r_A, r_B, x_A \cdot x_B \cdot P)$). We provide the description of the protocol from the full version of the paper [27] in which, according to the authors, minor errors were corrected compared to the original version. But the original version of the protocol can be considered as a separate protocol called TS1-2004.

For this protocol it is assumed that parties can be ordered by their identifiers (e.g., lexicographically) and we write "$A \prec B$" to denote this ordering.

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$r_A \xleftarrow{U} \{0,1\}^\lambda$	$\xrightarrow{A, r_A}$	
	$\xleftarrow{B, r_B}$	$r_B \xleftarrow{U} \{0,1\}^\lambda$
if $A \prec B$:		**if** $A \prec B$:
$src \leftarrow (A, B, r_A, r_B)$		$src \leftarrow (A, B, r_A, r_B)$
else :		**else** :
$src \leftarrow (B, A, r_B, r_A)$		$src \leftarrow (B, A, r_B, r_A)$
$K \leftarrow \mathsf{KDF}(src, x_A \cdot X_B)$		$K \leftarrow \mathsf{KDF}(src, x_B \cdot X_A)$
return K		**return** K

5.77 TS2

The original version of this protocol [26] does not assume including parties identifiers in the KDF function arguments during the session key computation ($K \leftarrow \mathsf{KDF}(E_A, E_B, e_A \cdot e_B \cdot P, x_A \cdot x_B \cdot P)$). As in 5.76, we provide the description of the protocol from the full version of the paper [27]. And again the original version of the protocol can be considered as a separate protocol called TS2-2004.

For this protocol it is assumed that parties can be ordered by their identifiers (e.g., lexicographically) and we write "$A \prec B$" to denote this ordering.

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, E_B}$	$E_B \leftarrow e_B \cdot P$
if $A \prec B$:		**if** $A \prec B$:
$src \leftarrow (A, B, E_A, E_B)$		$src \leftarrow (A, B, E_A, E_B)$
else :		**else** :
$src \leftarrow (B, A, E_B, E_A)$		$src \leftarrow (B, A, E_B, E_A)$
$K \leftarrow \mathsf{KDF}(src, e_A \cdot E_B, x_A \cdot X_B)$		$K \leftarrow \mathsf{KDF}(src, e_B \cdot E_A, x_B \cdot X_A)$
return K		**return** K

5.78 HC

$\mathbf{A}: (x_A, X_A), (x'_A, X'_A)$		$\mathbf{B}: (x_B, X_B), (x'_B, X'_B)$
$e_A \xleftarrow{U} \mathbb{Z}_q$		
$w_A \leftarrow \mathsf{H}(e_A, x_A, x'_A)$		
$W_A \leftarrow w_A \cdot P$	$\xrightarrow{A, W_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q$
		$w_B \leftarrow \mathsf{H}(e_B, x_B, x'_B)$
	$\xleftarrow{B, W_B}$	$W_B \leftarrow w_B \cdot P$
$Q_1 \leftarrow w_A \cdot (W_B + X_B)$		$Q_1 \leftarrow (w_B + x_B) \cdot W_A$
$Q_2 \leftarrow w_A \cdot (W_B + X'_B)$		$Q_2 \leftarrow (w_B + x'_B) \cdot W_A$
$Q_3 \leftarrow (w_A + x_A) \cdot W_B$		$Q_3 \leftarrow w_B \cdot (X_A + W_A)$
$Q_4 \leftarrow (w_A + x'_A) \cdot W_B$		$Q_4 \leftarrow w_B \cdot (X'_A + W_A)$
$src \leftarrow (W_A, W_B, A, B)$		$src \leftarrow (W_A, W_B, A, B)$
$K \leftarrow \mathsf{KDF}(Q_1, Q_2, Q_3, Q_4, src)$		$K \leftarrow \mathsf{KDF}(Q_1, Q_2, Q_3, Q_4, src)$
return K		**return** K

5.79 NAXOS+

$\mathbf{A}: x_A, X_A$		$\mathbf{B}: x_B, X_B$
$r_A \xleftarrow{U} \{0,1\}^\lambda$		
$w_A \leftarrow \mathsf{H}(r_A, x_A)$		
$W_A \leftarrow w_A \cdot P$	$\xrightarrow{A, W_A}$	$r_B \xleftarrow{U} \{0,1\}^\lambda$
		$w_B \leftarrow \mathsf{H}(r_B, x_B)$
	$\xleftarrow{B, W_B}$	$W_B \leftarrow w_B \cdot P$
$Q_1 \leftarrow x_A \cdot X_B$		$Q_1 \leftarrow x_B \cdot X_A$
$Q_2 \leftarrow x_A \cdot W_B$		$Q_2 \leftarrow w_B \cdot X_A$
$Q_3 \leftarrow w_A \cdot X_B$		$Q_3 \leftarrow x_B \cdot W_A$
$Q_4 \leftarrow w_A \cdot W_B$		$Q_4 \leftarrow w_B \cdot W_A$
$K \leftarrow \mathsf{KDF}(Q_1, Q_2, Q_3, Q_4, A, B)$		$K \leftarrow \mathsf{KDF}(Q_1, Q_2, Q_3, Q_4, A, B)$
return K		**return** K

5.80 NAXOS+1p

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$r_A \xleftarrow{U} \{0,1\}^\lambda$		
$w_A \leftarrow \mathsf{H}(r_A, x_A)$		
$W_A \leftarrow w_A \cdot P$	$\xrightarrow{A, W_A}$	
$K \leftarrow \mathsf{KDF}(x_A \cdot X_B, w_A \cdot X_B, A, B)$		$K \leftarrow \mathsf{KDF}(x_B \cdot X_A, x_B \cdot W_A, A, B)$
return K		**return** K

5.81 NAXOS+C

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$r_A \xleftarrow{U} \{0,1\}^\lambda$		
$w_A \leftarrow \mathsf{H}_1(r_A, x_A)$		
$W_A \leftarrow w_A \cdot P$	$\xrightarrow{A, W_A}$	$r_B \xleftarrow{U} \{0,1\}^\lambda$
		$w_B \leftarrow \mathsf{H}_1(r_B, x_B)$
		$W_B \leftarrow w_B \cdot P$
		$Q_1 \leftarrow x_B \cdot X_A$
		$Q_2 \leftarrow w_B \cdot X_A$
		$Q_3 \leftarrow x_B \cdot W_A$
		$Q_4 \leftarrow w_B \cdot W_A$
		$K^a \leftarrow \mathsf{KDF}(Q_1, Q_2, Q_3, Q_4, A, B)$
$Q_1 \leftarrow x_A \cdot X_B$	$\xleftarrow{B, W_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_1)$
$Q_2 \leftarrow x_A \cdot W_B$		
$Q_3 \leftarrow w_A \cdot X_B$		
$Q_4 \leftarrow w_A \cdot W_B$		
$K^a \leftarrow \mathsf{KDF}(Q_1, Q_2, Q_3, Q_4, A, B)$		
Verify τ_B		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_2)$	$\xrightarrow{\tau_A}$	Verify τ_A
$K \leftarrow \mathsf{KDF}(K^a)$		$K \leftarrow \mathsf{KDF}(K^a)$
return K		**return** K

5.82 FHMQV

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, B, E_A}$	Verify $\overline{B} = B$
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{E_B}$	$E_B \leftarrow e_B \cdot P$
$u \leftarrow \mathsf{H}(E_A, E_B, A, B)$		$u \leftarrow \mathsf{H}(E_A, E_B, A, B)$
$v \leftarrow \mathsf{H}(E_B, E_A, A, B)$		$v \leftarrow \mathsf{H}(E_B, E_A, A, B)$
$s_A \leftarrow e_A + u \cdot x_A$		$s_B \leftarrow e_B + v \cdot x_B$
$Q \leftarrow s_A \cdot (E_B + v \cdot X_B)$		$Q \leftarrow s_B \cdot (E_A + u \cdot X_A)$
$K \leftarrow \mathsf{KDF}(Q, A, B, E_A, E_B)$		$K \leftarrow \mathsf{KDF}(Q, A, B, E_A, E_B)$
return K		**return** K

5.83 FHMQV-C

$\mathbf{A}: x_A, X_A$		$\mathbf{B}: x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, B, E_A}$	Verify $\overline{B} = B$
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$u \leftarrow \mathsf{H}(E_A, E_B, A, B)$
		$v \leftarrow \mathsf{H}(E_B, E_A, A, B)$
		$s_B \leftarrow e_B + v \cdot x_B$
		$Q \leftarrow s_B \cdot (E_A + u \cdot X_A)$
		$K, K^a \leftarrow \mathsf{KDF}(Q, A, B, E_A, E_B)$
$u \leftarrow \mathsf{H}(E_A, E_B, A, B)$	$\xleftarrow{E_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(B, E_B)$
$v \leftarrow \mathsf{H}(E_B, E_A, A, B)$		
$s_A \leftarrow e_A + u \cdot x_A$		
$Q \leftarrow s_A \cdot (E_B + v \cdot X_B)$		
$K, K^a \leftarrow \mathsf{KDF}(Q, A, B, E_A, E_B)$		
Verify τ_B		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(A, E_A)$	$\xrightarrow{\tau_A}$	Verify τ_A
return K		**return** K

5.84 SIG-DH+

$\mathbf{A}: sk_A^s, pk_A^s$		$\mathbf{B}: sk_B^s, pk_B^s$
$e_A \xleftarrow{U} \mathbb{Z}_q$		
$w_A \leftarrow \mathsf{H}(e_A, sk_A^s)$		
$W_A \leftarrow w_A \cdot P$	$\xrightarrow{A, W_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q$
		$w_B \leftarrow \mathsf{H}(e_B, sk_B^s)$
		$W_B \leftarrow w_B \cdot P$
Verify σ_B	$\xleftarrow{B, W_B, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(B, W_B, W_A, A)$
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(A, W_A, W_B, B)$	$\xrightarrow{\sigma_A}$	Verify σ_A
$Q \leftarrow w_A \cdot W_B$		$Q \leftarrow w_B \cdot W_A$
$K \leftarrow \mathsf{KDF}(Q, W_A, W_B, A, B)$		$K \leftarrow \mathsf{KDF}(Q, W_A, W_B, A, B)$
return K		**return** K

5.85 SMQV

$\mathbf{A}: x_A, X_A$		$\mathbf{B}: x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, B, E_A}$	Verify $\overline{B} = B$
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{E_B}$	$E_B \leftarrow e_B \cdot P$
$u \leftarrow \mathsf{H}(E_A, E_B, A, B)$		$u \leftarrow \mathsf{H}(E_A, E_B, A, B)$
$v \leftarrow \mathsf{H}(E_B, E_A, A, B)$		$v \leftarrow \mathsf{H}(E_B, E_A, A, B)$
$s_A \leftarrow x_A + u \cdot e_A$		$s_B \leftarrow v \cdot e_B + x_B$
$Q \leftarrow s_A \cdot (v \cdot E_B + X_B)$		$Q \leftarrow s_B \cdot (u \cdot E_A + X_A)$
$K \leftarrow \mathsf{KDF}(Q, A, B, E_A, E_B)$		$K \leftarrow \mathsf{KDF}(Q, A, B, E_A, E_B)$
return K		**return** K

5.86 YAK

The original paper [41] introduces the family of YAK protocols with the arbitrary knowledge proof (KP) as the base cryptoprimitive. Since KP mechanism is not widely used by other protocols described in this paper, we do not introduce its general interface and describe the specific instance of YAK protocol, proposed in [41], with Schnorr signature used as the knowledge proof.

$\mathbf{A}: x_A, X_A$		$\mathbf{B}: x_B, X_B$
$e_A, e'_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$		
$E'_A \leftarrow e'_A \cdot P$		
$h \leftarrow \mathsf{H}(P, E'_A, E_A, A)$		
$s_A \leftarrow e'_A - e_A \cdot h$	$\xrightarrow{A, E_A, E'_A, s_A}$	$h \leftarrow \mathsf{H}(P, E'_A, E_A, A)$
		Verify $E'_A = s_A \cdot P + h \cdot E_A$
		$e_B, e'_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_A \cdot P$
		$E'_B \leftarrow e'_B \cdot P$
		$h' \leftarrow \mathsf{H}(P, E'_B, E_B, B)$
$h' \leftarrow \mathsf{H}(P, E'_B, E_B, B)$	$\xleftarrow{B, E_B, E'_B, s_B}$	$s_B \leftarrow e'_B - e_B \cdot h'$
Verify $E'_B = s_B \cdot P + h' \cdot E_B$		
$K \leftarrow \mathsf{KDF}((x_A + e_A) \cdot (E_B + X_B))$		$K \leftarrow \mathsf{KDF}((x_B + e_B) \cdot (E_A + X_A))$
return K		**return** K

5.87 EECKE-1N

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$Z_A \leftarrow e_A \cdot X_B$	$\xrightarrow{A, Z_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, Z_B}$	$Z_B \leftarrow e_B \cdot X_A$
$Q \leftarrow x_A^{-1} \cdot e_A \cdot Z_B$		$Q \leftarrow x_B^{-1} \cdot e_B \cdot Z_A$
$K \leftarrow \mathsf{KDF}(\mu(Q), \mu(Z_A), \mu(Z_B), A, B)$		$K \leftarrow \mathsf{KDF}(\mu(Q), \mu(Z_A), \mu(Z_B), A, B)$
return K		**return** K

5.88 TMQV

$\mathbf{A} : (x_A, X_A), (x'_A, X'_A)$		$\mathbf{B} : (x_B, X_B), (x'_B, X'_B)$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{B, A, E_A}$	Verify $\overline{B} = B$
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{E_B}$	$E_B \leftarrow e_B \cdot P$
$u \leftarrow \mathsf{H}(\mathsf{c}_1, A, B, E_A, E_B)$		$u \leftarrow \mathsf{H}(\mathsf{c}_1, A, B, E_A, E_B)$
$v \leftarrow \mathsf{H}(\mathsf{c}_2, B, A, E_B, E_A)$		$v \leftarrow \mathsf{H}(\mathsf{c}_2, B, A, E_B, E_A)$
$s_A \leftarrow e_A + u \cdot x_A$		$s_B \leftarrow e_B + v \cdot x_B$
$s'_A \leftarrow e_A + u \cdot x'_A$		$s'_B \leftarrow e_B + v \cdot x'_B$
$Q_1 \leftarrow s_A \cdot (E_B + v \cdot X_B)$		$Q_1 \leftarrow s_B \cdot (E_A + u \cdot X_A)$
$Q_2 \leftarrow s'_A \cdot (E_B + v \cdot X'_B)$		$Q_2 \leftarrow s'_B \cdot (E_A + u \cdot X'_A)$
$K \leftarrow \mathsf{KDF}(Q_1, Q_2, A, B, E_A, E_B)$		$K \leftarrow \mathsf{KDF}(Q_1, Q_2, A, B, E_A, E_B)$
return K		**return** K

5.89 CF

$\mathbf{A}: (x_A, X_A), (sk_A^s, pk_A^s)$		$\mathbf{B}: (x_B, X_B), (sk_B^s, pk_B^s)$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_A)$	$\xrightarrow{A, E_A, \sigma_A}$	Verify σ_A
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
Verify σ_B	$\xleftarrow{B, E_B, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_B)$
$W \leftarrow (e_A + x_A) \cdot (E_B + X_B)$		$W \leftarrow (e_B + x_B) \cdot (E_A + X_A)$
$K \leftarrow \mathsf{KDF}(A, B, W, E_A)$		$K \leftarrow \mathsf{KDF}(A, B, W, E_A)$
return K		**return** K

5.90 CMQV+

$\mathbf{A}: x_A, X_A$		$\mathbf{B}: x_B, X_B$
$r_A \xleftarrow{U} \{0,1\}^\lambda$		
$w_A \leftarrow \mathsf{H}_1(r_A, x_A)$		
$W_A \leftarrow w_A \cdot P$	$\xrightarrow{B, A, W_A}$	Verify $\overline{B} = B$
		$r_B \xleftarrow{U} \{0,1\}^\lambda$
		$w_B \leftarrow \mathsf{H}_1(r_B, x_B)$
	$\xleftarrow{W_B}$	$W_B \leftarrow w_B \cdot P$
$u \leftarrow \mathsf{H}_2(W_B, A, B)$		$u \leftarrow \mathsf{H}_2(W_B, A, B)$
$V \leftarrow W_B + u \cdot X_B$		$v \leftarrow w_B + u \cdot x_B$
$Q_1 \leftarrow x_A \cdot V$		$Q_1 \leftarrow v \cdot X_A$
$Q_2 \leftarrow w_A \cdot V$		$Q_2 \leftarrow v \cdot W_A$
$K \leftarrow \mathsf{KDF}(Q_1, Q_2, W_A, W_B, A, B)$		$K \leftarrow \mathsf{KDF}(Q_1, Q_2, W_A, W_B, A, B)$
return K		**return** K

5.91 GC

The original paper introduces GC protocol with specific function used for key derivation. Following the guidelines of the protocol description, we define GC protocol with the general KDF function.

$\mathbf{A} : (sk_A^k, pk_A^k), K_A^p, S_A$		$\mathbf{B} : (sk_B^k, pk_B^k), K_B^p, S_B$
$r_A \xleftarrow{U} \{0,1\}^\lambda, \widetilde{K_A^p} \xleftarrow{U} \mathcal{K}_p$		
$rnd_A \leftarrow \mathsf{PRF}^1_{K_A^p}(r_A) \oplus \mathsf{PRF}^2_{\widetilde{K_A^p}}(S_A)$		
$C_A, K_A \leftarrow \mathcal{KEM}_1.\mathsf{Encaps}_{pk_B^k}(rnd_A)$		
$(\widetilde{sk_A^k}, \widetilde{pk_A^k}) \leftarrow \mathcal{KEM}_2.\mathsf{KGen}(\ )$	$\xrightarrow{A, B, C_A, \widetilde{pk_A^k}}$	Verify $\overline{B} = B$
		$r_B \xleftarrow{U} \{0,1\}^\lambda, \widetilde{K_B^p} \xleftarrow{U} \mathcal{K}_p$
		$rnd_B \leftarrow \mathsf{PRF}^1_{K_B^p}(r_B) \oplus \mathsf{PRF}^2_{\widetilde{K_B^p}}(S_B)$
		$C_B, K_B \leftarrow \mathcal{KEM}_1.\mathsf{Encaps}_{pk_A^k}(rnd_B)$
$K_B \leftarrow \mathcal{KEM}_1.\mathsf{Decaps}_{sk_A^k}(C_B)$	$\xleftarrow{C_B, C'_B}$	$C'_B, K'_B \leftarrow \mathcal{KEM}_2.\mathsf{Encaps}_{\widetilde{pk_A^k}}(\ )$
$K'_B \leftarrow \mathcal{KEM}_2.\mathsf{Decaps}_{\widetilde{sk_A^k}}(C'_B)$		$K_A \leftarrow \mathcal{KEM}_1.\mathsf{Decaps}_{sk_B^k}(C_A)$
$src_1 \leftarrow (A, B, pk_A^k, pk_B^k)$		$src_1 \leftarrow (A, B, pk_A^k, pk_B^k)$
$src_2 \leftarrow (C_A, \widetilde{pk_A^k}, C_B, C'_B)$		$src_2 \leftarrow (C_A, \widetilde{pk_A^k}, C_B, C'_B)$
$K \leftarrow \mathsf{KDF}(K_A, K_B, K'_B, src_1, src_2)$		$K \leftarrow \mathsf{KDF}(K_A, K_B, K'_B, src_1, src_2)$
return K		**return** K

5.92 sHMQV

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{B, E_B}$	$E_B \leftarrow e_B \cdot P$
$d \leftarrow \mathsf{H}(E_A, B, E_B)$		$d \leftarrow \mathsf{H}(E_A, B, E_B)$
$e \leftarrow \mathsf{H}(E_B, A, E_A)$		$e \leftarrow \mathsf{H}(E_B, A, E_A)$
$s_A \leftarrow e_A + d \cdot x_A$		$s_B \leftarrow e_B + e \cdot x_B$
$Q \leftarrow s_A \cdot (E_B + e \cdot X_B)$		$Q \leftarrow s_B \cdot (E_A + d \cdot X_A)$
$K \leftarrow \mathsf{KDF}(Q, A, B, E_A, E_B)$		$K \leftarrow \mathsf{KDF}(Q, A, B, E_A, E_B)$
return K		**return** K

5.93 Echinacea-3

$\mathbf{A} : (sk_A^s, pk_A^s), \mathsf{info}$		$\mathbf{B} : (sk_B^s, pk_B^s), \mathsf{info}$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A, A, B, \mathsf{sid})$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_B, E_A, A)$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot E_B, A, B, \mathsf{sid})$	$\xleftarrow{B, E_B, \sigma_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_1, E_B, E_A, B, A)$
Verify σ_B, τ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_A, E_B, B)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_2, E_A, E_B, A, B)$	$\xrightarrow{\sigma_A, \tau_A}$	Verify σ_A, τ_A
return K		**return** K

5.94 Echinacea-3-psk

$\mathbf{A}$: (sk_A^s, pk_A^s), sid, psk		$\mathbf{B}$: (sk_B^s, pk_B^s), sid, psk
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$ $K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A, A, B, \mathsf{sid}, \mathsf{psk})$ $\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_B, E_A, A)$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot E_B, A, B, \mathsf{sid}, \mathsf{psk})$	$\xleftarrow{B, E_B, \sigma_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_1, E_B, E_A, B, A)$
Verify σ_B, τ_B $\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_A, E_B, B)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_2, E_A, E_B, A, B)$	$\xrightarrow{\sigma_A, \tau_A}$	Verify σ_A, τ_A
return K		**return** K

5.95 Echinacea-2

$\mathbf{A}$: sid		$\mathbf{B}$: (sk_B^s, pk_B^s), sid
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$ $K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A, A, B, \mathsf{sid})$ $\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_B, E_A, A)$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot E_B, A, B, \mathsf{sid})$	$\xleftarrow{B, E_B, \sigma_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_1, E_B, E_A, B, A)$
Verify σ_B, τ_B		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_2, E_A, E_B, A, B)$	$\xrightarrow{\tau_A}$	Verify τ_A
return K		**return** K

5.96 Echinacea-2-psk

$\mathbf{A}$: sid, psk		$\mathbf{B}$: (sk_B^s, pk_B^s), sid, psk
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A, A, B, \mathsf{sid}, \mathsf{psk})$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_B, E_A, A)$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot E_B, A, B, \mathsf{sid}, \mathsf{psk})$	$\xleftarrow{B, E_B, \sigma_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_1, E_B, E_A, B, A)$
Verify σ_B, τ_B		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_2, E_A, E_B, A, B)$	$\xrightarrow{\tau_A}$	Verify τ_A
return K		**return** K

5.97 Limonnik-3

This protocol allows the usage of two (possibly different) elliptic curves for calculating Diffie-Hellman values. Since it does not affect the cryptographic core of the protocol, we describe the particular case of Limonnik-3 with one curve.

$\mathbf{A}$: (x_A, X_A), sid		$\mathbf{B}$: (x_B, X_B), sid
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K^* \leftarrow e_B \cdot X_A$
		$Z \leftarrow x_B \cdot E_A$
		$K, K^a \leftarrow \mathsf{KDF}(K^*, Z, A, B, \mathsf{sid})$
$K^* \leftarrow x_A \cdot E_B$	$\xleftarrow{B, E_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_1, E_B, E_A, B, A)$
$Z \leftarrow e_A \cdot X_B$		
$K, K^a \leftarrow \mathsf{KDF}(K^*, Z, A, B, \mathsf{sid})$		
Verify τ_B		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_2, E_A, E_B, A, B)$	$\xrightarrow{\tau_A}$	Verify τ_A
return K		**return** K

5.98 Limonnik-3-psk

$\mathbf{A} : (x_A, X_A), \mathsf{sid}, \mathsf{psk}$		$\mathbf{B} : (x_B, X_B), \mathsf{sid}, \mathsf{psk}$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, E_A}$	$e_B \xleftarrow{U} \mathbb{Z}_q^*$
		$E_B \leftarrow e_B \cdot P$
		$K^* \leftarrow e_B \cdot X_A$
		$Z \leftarrow x_B \cdot E_A$
		$K, K^a \leftarrow \mathsf{KDF}(K^*, Z, A, B, \mathsf{sid}, \mathsf{psk})$
$K^* \leftarrow x_A \cdot E_B$	$\xleftarrow{B, E_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_1, E_B, E_A, B, A)$
$Z \leftarrow e_A \cdot X_B$		
$K, K^a \leftarrow \mathsf{KDF}(K^*, Z, A, B, \mathsf{sid}, \mathsf{psk})$		
Verify τ_B		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_2, E_A, E_B, A, B)$	$\xrightarrow{\tau_A}$	Verify τ_A
return K		**return** K

5.99 eFHMQV

$\mathbf{A} : x_A, X_A$		$\mathbf{B} : x_B, X_B$
$e_A \xleftarrow{U} \mathbb{Z}_q^*$		
$E_A \leftarrow e_A \cdot P$	$\xrightarrow{A, B, E_A}$	Verify $\overline{B} = B$
		$e_B \xleftarrow{U} \mathbb{Z}_q^*$
	$\xleftarrow{E_B}$	$E_B \leftarrow e_B \cdot P$
$u \leftarrow \mathsf{H}(E_A, E_B, X_A, A, X_B, B)$		$u \leftarrow \mathsf{H}(E_A, E_B, X_A, A, X_B, B)$
$v \leftarrow \mathsf{H}(E_B, E_A, X_A, A, X_B, B)$		$v \leftarrow \mathsf{H}(E_B, E_A, X_A, A, X_B, B)$
$s_A \leftarrow e_A + u \cdot x_A$		$s_B \leftarrow e_B + v \cdot x_B$
$Q \leftarrow s_A \cdot (E_B + v \cdot X_B)$		$Q \leftarrow s_B \cdot (E_A + u \cdot X_A)$
$K \leftarrow \mathsf{KDF}(Q, X_A, A, X_B, B, E_A, E_B)$		$K \leftarrow \mathsf{KDF}(Q, X_A, A, X_B, B, E_A, E_B)$
return K		**return** K

5.100 $\mathcal{C}_{\mathsf{SigMA}}$

$\mathbf{A}: sk^s_A, pk^s_A$		$\mathbf{B}: sk^s_B, pk^s_B$
$(sk^k_A, pk^k_A) \leftarrow \mathcal{KEM}.\mathsf{KGen}(\,)$	$\xrightarrow{pk^k_A}$	$C, K' \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{pk^k_A}(\,)$
$K' \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{sk^k_A}(C)$	$\xleftarrow{C}$	
$src \leftarrow (pk^k_A, C)$		$src \leftarrow (pk^k_A, C)$
$K^a \leftarrow \mathsf{KDF}(K', \mathsf{c}_1, src)$		$K^a \leftarrow \mathsf{KDF}(K', \mathsf{c}_1, src)$
$r_A \xleftarrow{U} \{0,1\}^\lambda$	$\xrightarrow{r_A}$	$r_B \xleftarrow{U} \{0,1\}^\lambda$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk^s_B}(\mathsf{c}_2, src, r_A, r_B)$
Verify σ_B, τ_B	$\xleftarrow{B, r_B, \sigma_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_2, B)$
$\sigma_A \leftarrow \mathsf{Sig}_{sk^s_A}(\mathsf{c}_3, src, r_A, r_B)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(\mathsf{c}_3, A)$	$\xrightarrow{A, \sigma_A, \tau_A}$	Verify σ_A, τ_A
$K \leftarrow \mathsf{KDF}(K', \mathsf{c}_4, src, r_A, r_B, A, B)$		$K \leftarrow \mathsf{KDF}(K', \mathsf{c}_4, src, r_A, r_B, A, B)$
return K		**return** K

6 Conclusion

Current version of this paper is just the first step in a long process of counting all the existing AKE protocols. We hope that even the results obtained up to now may inspire the reader to give us feedback on the principles of protocol description. We will address the comments received from the crypto community in the next versions of the paper.

The authors thank Liliya Akhmetzyanova, Andrey Bozhko and Sergey Kyazhin for their valuable comments.

References

[1] Diffie W., Hellman M. «New directions in cryptography». IEEE Transactions on Information Theory, 22(6), pp. 644–654, 1976.

[2] Matsumoto T., Takashima Y., Imai H. «On Seeking Smart Public-key Distribution Systems». Transactions of the IECE of Japan, E69, pp. 99–106, 1986.

[3] Diffie W., Van Oorschot P.C., Wiener M.J. «Authentication and authenticated key exchanges». Designs, Codes and cryptography, 2(2), pp. 107–125, 1992.

[4] ISO/IEC IS 9798-3, «Entity authentication mechanisms — Part 3: Entity authentication using asymmetric techniques», 1993.

[5] Nyberg K., Rueppel R.A. «Message recovery for signature schemes based on the discrete logarithm problem». Workshop on the Theory and Application of Cryptographic Techniques, pp. 182–193, 1994.

[6] Menezes A.J., Qu M., Vanstone S.A. «Some new key agreement protocols providing implicit authentication». Workshop on Selected Areas in Cryptography (SAC'95), pp. 22–32, 1995.

[7] Lowe G. «Breaking and fixing the Needham-Schroeder public-key protocol using FDR». International Workshop on Tools and Algorithms for the Construction and Analysis of Systems, pp. 147–166, 1996.

[8] Menezes A.J., Van Oorschot P.C., Vanstone S.A. «Handbook of applied cryptography». CRC press, 1996.

[9] Nyberg K., Rueppel R.A. «Message recovery for signature schemes based on the discrete logarithm problem». Designs, Codes and Cryptography, 7(1), pp. 61–81, 1996.

[10] Blake-Wilson S., Johnson D., Menezes A. «Key Agreement Protocols and their Security Analysis». 6th IMA International Conference on Cryptography and Coding, LNCS 1355, pp. 30-45, Springer-Verlag, 1997.

[11] Blake-Wilson S., Menezes A. «Entity authentication and authenticated key transport protocols employing asymmetric techniques». International Workshop on Security Protocols, pp. 137–158. 1997.

[12] NIST, «SKIPJACK and KEA Algorithm Specification», `http://csrc.nist.gov/encryption/skipjack/skipjack.pdf`, 1998.

[13] Law L., Menezes A.J., Qu M., Solinas J., Vanstone S. «An efficient protocol for authenticated key agreement». Tech. Rep. CORR 98-05, Department of C&O, University of Waterloo, 1998.

[14] Lee C., Lim J., Kim J. «An efficient and secure key agreement». IEEE p1363a draft, 1998.

[15] Karn P., Simpson W. «Photuris: Session-key management protocol». RFC 2522, 1999.

[16] Shoup V. «On formal models for secure key exchange». Cryptology ePrint Archive, Paper 1999/012, 1999.

[17] Song B., Kim K. «Two-Pass Authenticated Key Agreement Protocol with Key Confirmation». INDOCRYPT 2000, LNCS 1977, pp. 237–249, 2000.

[18] Canetti R., Krawczyk H. «Analysis of key-exchange protocols and their use for building secure channels (Full Version)». Cryptology ePrint Archive, Paper 2001/040, 2001.

[19] Harn L., Lin H. Y. «Authenticated key agreement without using one-way hash functions». Electronics Letters, 37(10), pp. 629–630, 2001.

[20] Krawczyk H. «SIGMA: The 'SIGn-and-MAc' Approach to Authenticated Diffie-Hellman and its Use in the IKE Protocols». CRYPTO'03, LNCS 2729, pp. 400–425, 2003.

[21] Law L., Menezes A.J., Qu M., Solinas J., Vanstone S. «An efficient protocol for authenticated key agreement». Designs, Codes and Cryptography, 28(2), pp. 119–134, 2003.

[22] Aiello W., Bellovin S.M., Blaze M., Canetti R., Ioannidis J., Keromytis A.D., Reingold O. «Efficient, DoS-Resistant, Secure Key Exchange for Internet Protocols». Proceedings of the ACM Computer and Communications Security (CCS) Conference, pp. 48–58, 2003.

[23] Al-Sultan K., Saeb M., Elmessiery M., Badawi U.A. «A new two-pass key agreement protocol». 46th Midwest Symposium on Circuits and Systems, 1, pp. 509–511, 2003.

[24] Popescu C. «A secure authenticated key agreement protocol». Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference (IEEE Cat. No.04CH37521), 2, pp. 783–786, 2004.

[25] Aiello W., Bellovin S.M., Blaze M., Canetti R., Ioannidis J., Keromytis A.D., Reingold O. «Just fast keying: Key agreement in a hostile internet». ACM Trans. Inf. Syst. Secur, 7(2), pp. 242–273, 2004.

[26] Jeong I.R., Katz J., Lee D.H. «One-Round Protocols for Two-Party Authenticated Key Exchange». Applied Cryptography and Network Security, ACNS 2004, LNCS 3089, pp. 220–232, 2004.

[27] Jeong I.R., Katz J., Lee D.H. «One-Round Protocols for Two-Party Authenticated Key Exchange». 2008. `https://www.cs.umd.edu/~jkatz/papers/1round_AKE.pdf`

[28] Krawczyk H. «HMQV: A high-performance secure Diffie-Hellman protocol». Annual international cryptology conference, pp. 546–566, 2005.

[29] Lauter K., Mityagin A. «Security Analysis of KEA Authenticated Key Exchange Protocol». Cryptology ePrint Archive, Paper 2005/265, 2005.

[30] Strangio M.A. «Efficient Diffie–Hellman two-party key agreement protocols based on elliptic curves». Proc. 20th ACM Symposium on Applied Computing (SAC), pp. 324–331, 2005.

[31] LaMacchia B.A., Lauter K., Mityagin A. «Stronger security of authenticated key exchange». Cryptology ePrint Archive, Paper 2006/073, 2006.

[32] Jeong I.R., Kwon J.O., Lee D.H. «A Diffie-Hellman Key Exchange Protocol Without Random Oracles». Cryptology and Network Security, CANS 2006, LNCS 4301, pp. 37–54, 2006.

[33] Ustaoglu B. «Obtaining a secure and efficient key agreement protocol from (H) MQV and NAXOS». Designs, Codes and Cryptography, 46(3), pp. 329–342, 2008.

[34] Wang S., Cao Z., Strangio M.A., Wang L. «Cryptanalysis and Improvement of an Elliptic Curve Diffie-Hellman Key Agreement Protocol». Cryptology ePrint Archive, Paper 2007/026, 2007.

[35] Huang H., Cao Z. «Strongly Secure Authenticated Key Exchange Protocol Based on Computational Diffie-Hellman Problem». Cryptology ePrint Archive, Paper 2008/500, 2008.

[36] Lee J., Park J.H. «Authenticated Key Exchange Secure under the Computational Diffie-Hellman Assumption». Cryptology ePrint Archive, Paper 2008/344, 2008.

[37] Sarr A.P., Elbaz-Vincent P., Bajard J.C. «A secure and efficient authenticated Diffie–Hellman protocol». European Public Key Infrastructure Workshop, pp. 83–98, 2009.

[38] Ustaoglu B. «Obtaining a secure and efficient key agreement protocol from (H)MQV and NAXOS (extended version)». Cryptology ePrint Archive, Paper 2007/123, 2009.

[39] Huang H., Cao Z. «Authenticated Key Exchange Protocols with Enhanced Freshness Properties». Cryptology ePrint Archive, Paper 2009/505, 2009.

[40] Sarr A.P., Elbaz-Vincent P., Bajard J.C. «Enhanced Security and Efficiency for Authenticated Key Agreement». Workshop on Foundations of Security and Privacy, FCS-PrivMod 2010, 2010.

[41] Hao F. «On Robust Key Agreement Based on Public Key Authentication». Cryptology ePrint Archive, Paper 2010/136, 2010.

[42] Yooni E.J., Yoo K.Y. «A new elliptic curve diffie-hellman two-party key agreement protocol». 2010 7th International Conference on Service Systems and Service Management, pp. 1–4, 2010.

[43] Pan J., Wang L. «TMQV: A Strongly eCK-Secure Diffie-Hellman Protocol without Gap Assumption». Provable Security, ProvSec 2011, LNCS 6980, pp. 380–388, 2011.

[44] Cremers C., Feltz M. «One-round Strongly Secure Key Exchange with Perfect Forward Secrecy and Deniability». Cryptology ePrint Archive, Paper 2011/300, 2011.

[45] Li H., Wu C.K. «CMQV+: An authenticated key exchange protocol from CMQV». Science China Information Sciences, 55(7), pp. 1666–1674, 2012.

[46] Fujioka, A., Suzuki, K., Xagawa, K., Yoneyama, K. «Strongly Secure Authenticated Key Exchange from Factoring, Codes, and Lattices». Cryptology ePrint Archive, Paper 2012/211, 2012.

[47] Basin D., Cremers C., Horvat M. «Actor key compromise: Consequences and countermeasures». IEEE 27th Computer Security Foundations Symposium, pp. 244–258, 2014.

[48] Zhao S., Zhang Q. «sHMQV: An Efficient Key Exchange Protocol for Power-limited Devices». Cryptology ePrint Archive, Paper 2015/110, 2015.

[49] ISO/IEC 11770-3, «Information Technology — Security Techniques — Key management — Part 3: Mechanisms using asymmetric techniques», 3rd edn. International Standard. 2015.

[50] Donenfeld J.A. «Wireguard: next generation kernel network tunnel». NDSS, pp. 1–12, 2017.

[51] Federal Agency on Technical Regulating and Metrology. «Information technology. Cryptographic data security. Shared key generating schemes with authentication using public key». R 1323565.1.004-2017, (in Russian), 2017.

[52] Seye P.B., Sarr A.P. «Enhanced Modelling of Authenticated Key Exchange Security». Security and Trust Management, STM 2017, LNCS 10547, pp. 36–52, 2017.

[53] Bindel N., Brendel J., Fischlin M., Goncalves B., Stebila, D. «Hybrid key encapsulation mechanisms and authenticated key exchange». Post-Quantum Cryptography: 10th International Conference, PQCrypto 2019, 2019 Revised Selected Papers 10, pp. 206–226, 2019.

[54] Boyd C., Mathuria A., Stebila D. «Protocols for Authentication and Key Establishment». 2020.

[55] Kaliski B. «An Unknown Key-Share Attack on the MQV Key Agreement Protocol». ACM Trans. Inf. Syst. Secur., 4, pp. 275–288, 2001.

[56] Chen L., Cheng Z., Smart N.P.: «Identity-based key agreement protocols from pairings». International Journal of Information Security, 6, 213–241, 2007.

[57] Kolesnikov V., Sundaram G.S. «IBAKE: Identity-Based Authenticated Key Exchange Protocol». Cryptology ePrint Archive, Paper 2011/612, 2011.

[58] Stickel E. «A new method for exchanging secret keys». Third International Conference on Information Technology and Applications, ICITA'05, 2, pp. 426–430, 2005.

[59] De Feo L., Jao D., Plut J. «Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies». Cryptology ePrint Archive, Paper 2011/506, 2011.

[60] Grigoriev D., Shpilrain V. «Tropical cryptography». Comm. Algebra, 42(6), pp. 2624–2632, 2014.

[61] Zhang J., Zhang Z., Ding J., Snook M., Dagdelen O. «Authenticated key exchange from ideal lattices». EUROCRYPT 2015, LNCS 9057, pp. 719–751, 2015.

[62] Grigoriev D., Shpilrain V. «Tropical cryptography II: extensions by homomorphisms». Comm. Algebra, 47(10), pp. 4224–4229, 2019.

[63] Ingemarsson I., Tang D.T., Wong C.K. «A Conference Key Distribution System». IEEE Transactions on Information Theory, 28(5), pp. 714–720, 1982.

[64] Burmester M., Desmedt Y. «A Secure and Efficient Conference Key Distribution System». EUROCRYPT 1994, LNCS 950, pp. 275–286, 1995.

[65] Kim Y., Perrig A., Tsudik G. «Communication-Efficient Group Key Agreement». Proc. IFIP TC11 16th Annual Working Conference on Information Security (IFIP/SEC), pp. 229–244, 2001.

[66] Smyshlyaev S.V., Alekseev E.K., Oshkin I.B., Popov V.O. «The security evaluated standardized password authenticated key exchange (SESPAKE) protocol». RFC 8133, 2017.

[67] Harkins D. «Dragonfly Key Exchange». RFC 7664, 2015.

[68] Bellare M., Pointcheval D., Rogaway P. «Authenticated key exchange secure against dictionary attacks». Cryptology ePrint Archive, Paper 2000/014, 2000.

[69] Brown D., Menezes A. «A Small Subgroup Attack on a Key Agreement Protocol of Arazi». Bulletin of the ICA, 37, pp. 45–50, 2003.

[70] Biehl I., Meyer B., Muller V. «Differential Fault Attacks on Elliptic Curve Cryptosystems». CRYPTO 2000, LNCS 1880, pp. 131–146, 2000.

[71] Jager T., Schwenk J., Somorovsky J. «Practical Invalid Curve Attacks on TLS-ECDH». Computer Security, ESORICS 2015, LNCS 9326, pp. 407–425, 2015.

[72] Alekseev E.K., Kyazhin S.N., Smyshlyaev S.V. «The Threat of Forcing the Identical Roles for Authenticated Key Establishment Protocols». J Comput Virol Hack Tech, pp. 1–6, 2023.

[73] Mavrogiannopoulos N., Vercauteren F., Velichkov V., Preneel B. «A cross-protocol attack on the TLS protocol». 2012 ACM Conference in Computer and Communications Security, pp. 62–72, 2012.