An Introduction of CPSEC and My Research Fields

(Authentication and Key Exchange Protocols)

SeongHan Shin

Cyber Physical Security Research Center (CPSEC),

National Institute of Advanced Industrial Science and Technology (AIST), Japan

국민대학교 정보보안연구소 특강

May 30th, 2023

Contents

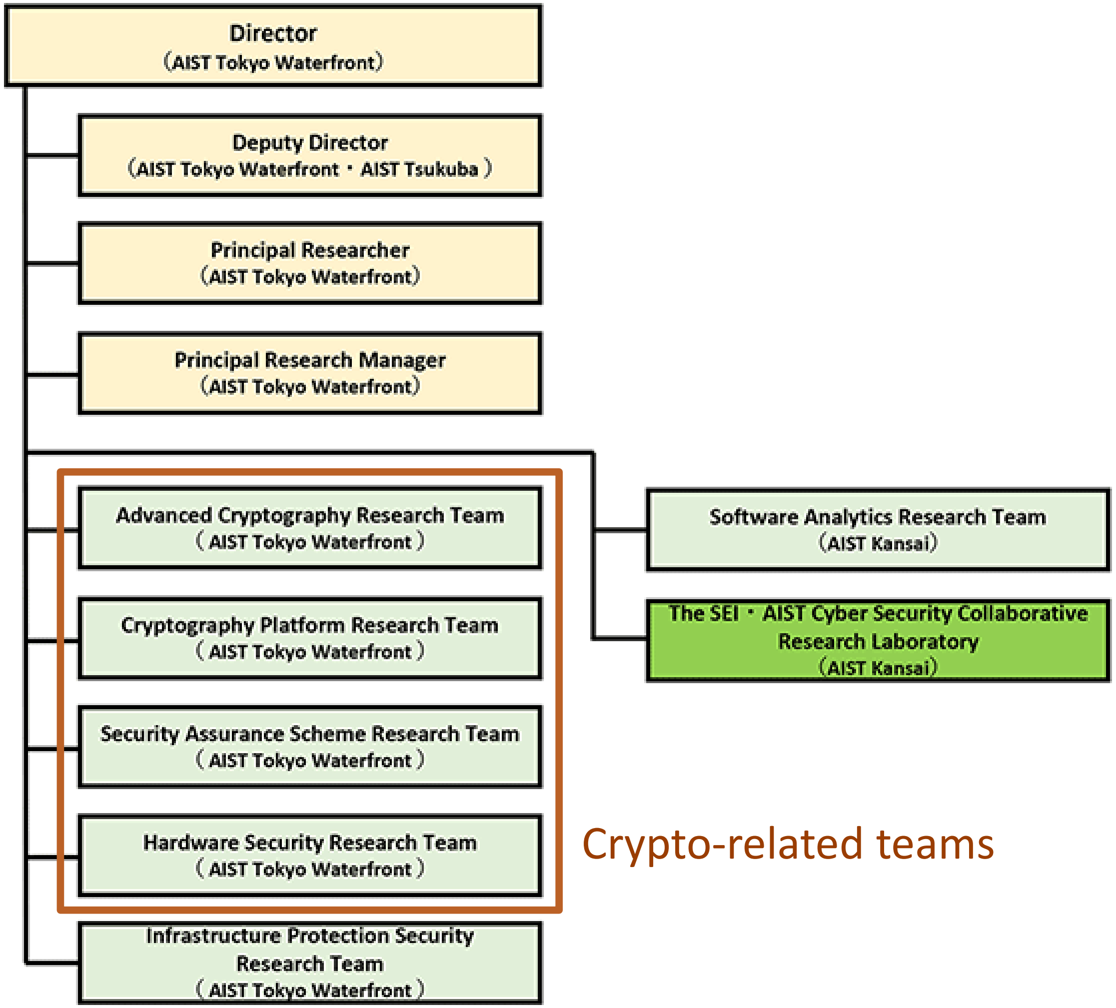
- Introduction of CPSEC
- My Research Fields
  - Authenticated Key Exchange
  - Password based AKE
  - Password-Authenticated Key Exchange
  - Anonymous PAKE
  - Leakage-Resilient AKE
  - Hybrid AKE
  - Applications

Introduction of CPSEC

CPSEC for Cyber-Physical Security

- Duration: From November 2018 to March 2025
- Director: Prof. T. Matsumoto (Yokohama National University)
  - Using cross-appointment system
- Structure: 6 research teams
  - Cryptography, hardware/software security, security assurance, ...
- Number of members: 120
  - Including visitors, students and administrative staffs
- Mission
  - Supporting government measures for supply/value chain security from technical viewpoints
  - Conducting research to make security measurable
  - Accumulating latest technology and knowledge
- https://www.cpsec.aist.go.jp/index_en.html

Organization (As of April 1, 2022)

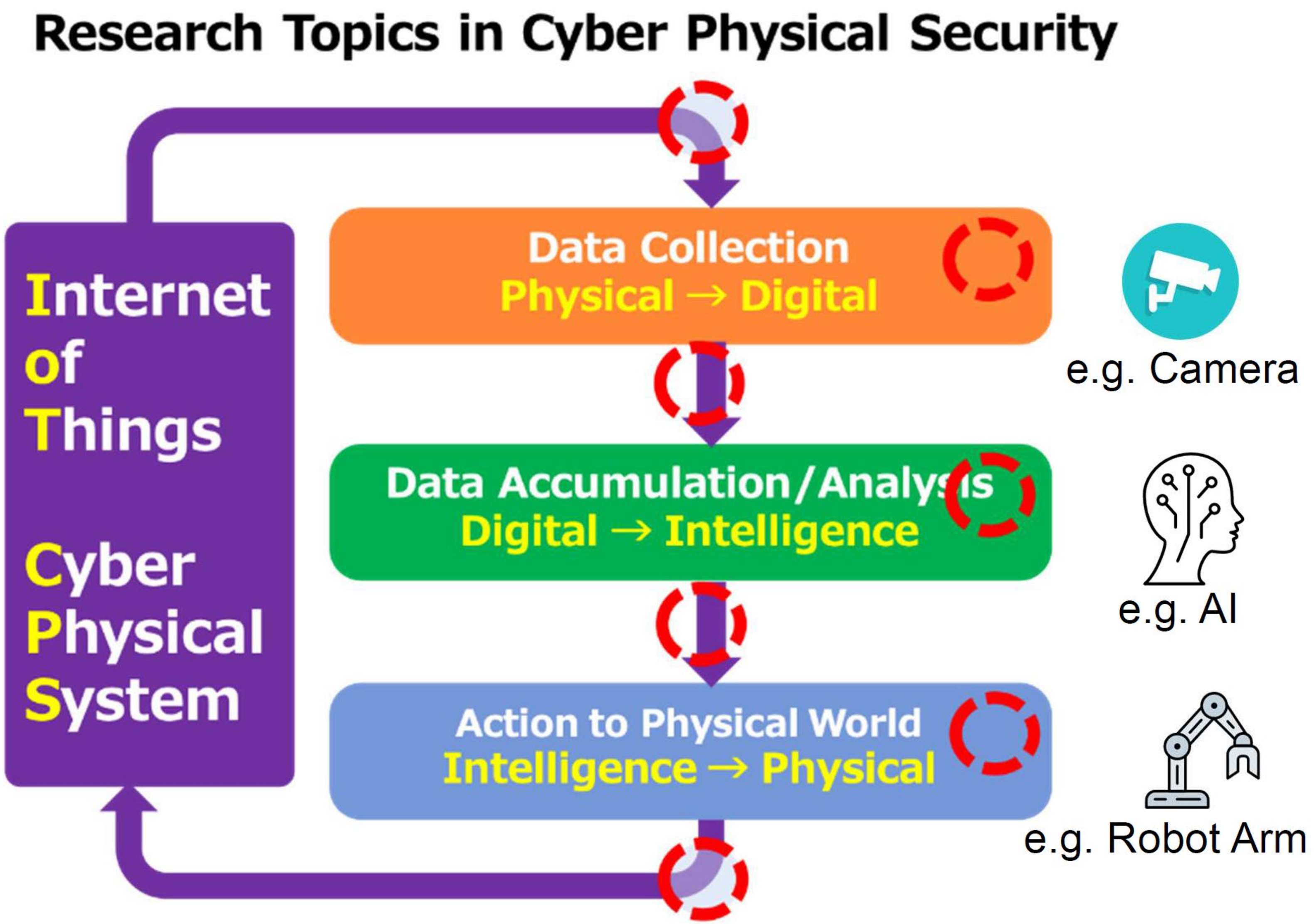



AIST Tokyo Waterfront

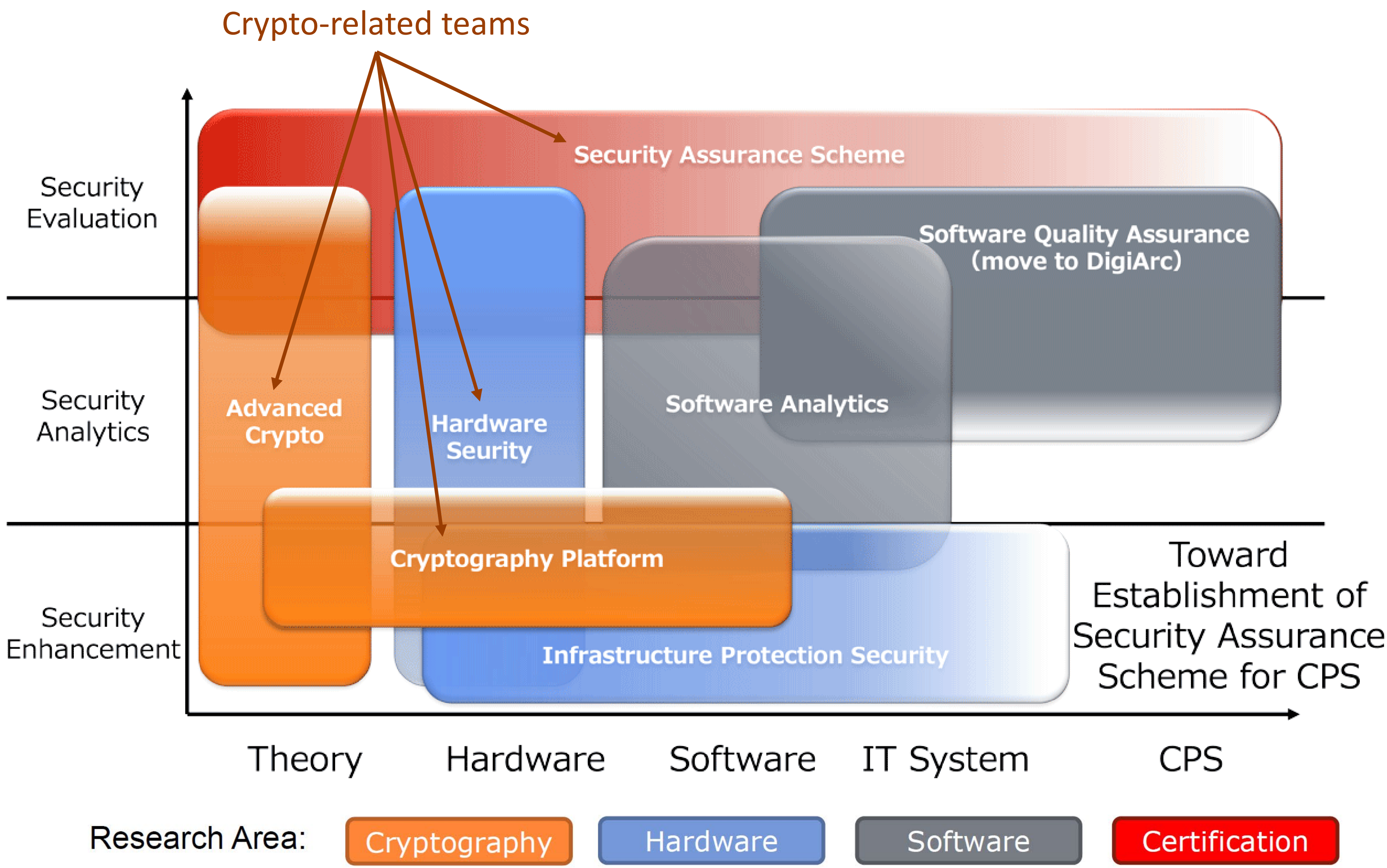

AIST Tsukuba


AIST Kansai

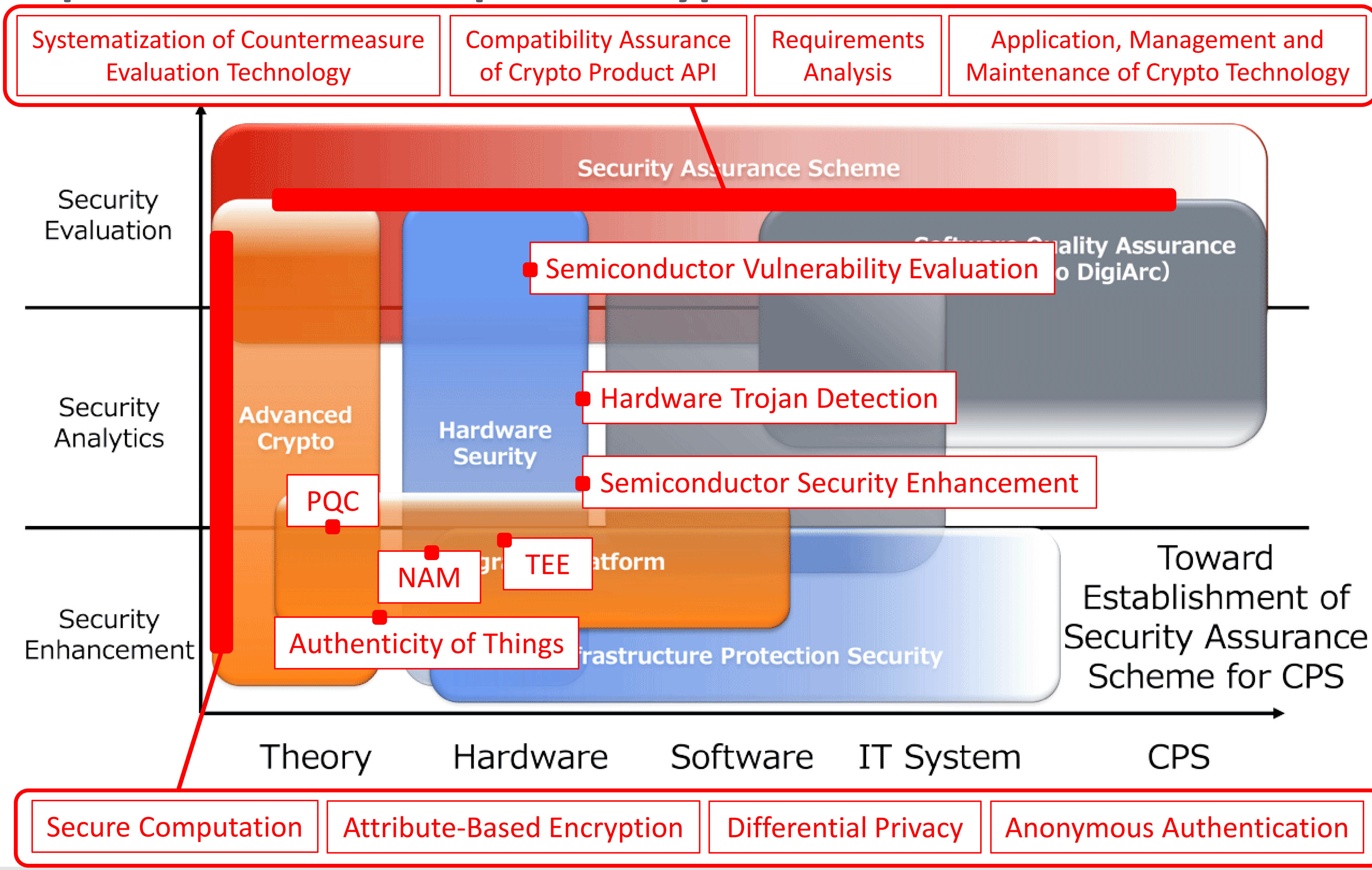
Attack points (red circles) are everywhere in CPS



Relationship between research topics and teams



Specific research topics of crypto-related teams



My Research Fields

Notation

- $E_{PK\_A}(M)$: public-key encryption of message M with public-key of A such that $D_{SK\_A}(E_{PK\_A}(M))=M$
- $SE_K(M)$: symmetric-key encryption of message M with key K such that $SD_K(SE_K(M))=M$
- $Sig_{SK\_A}(M)$: signature of message M generated by A such that $Verify_{PK\_A}(Sig_{SK\_A}(M))=accept$
- $MAC_K(M)$: message authentication code of message M using key K such that $Verify_K(MAC_K(M))=accept$
- H(M): one-way hash function of message M

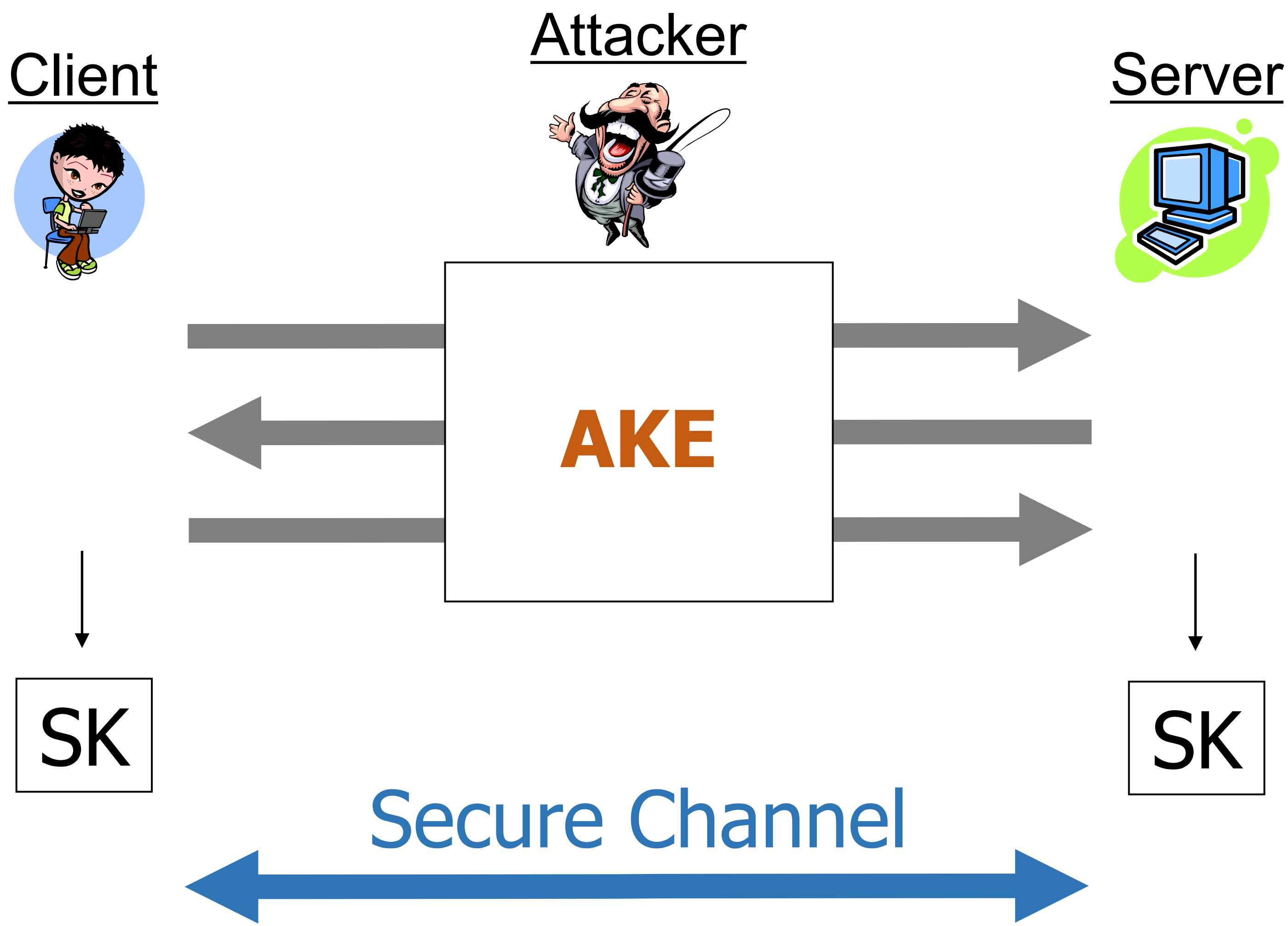
Authenticated Key Exchange

Authenticated Key Exchange [DOW92]

- Authentication + key exchange
- "… Key exchange should be linked to authentication so that a party has assurances that an exchanged key (which might be used to facilitate privacy or integrity and thus keep authenticity alive) is in fact shared with the authenticated party, and not an impostor. …"

[DOW92] W. Diffie, P. C. van Oorschot, and M. J. Wiener, "Authentication and Authenticated Key Exchanges," Designs, Codes and Cryptography, 1992

Authenticated Key Exchange (AKE)



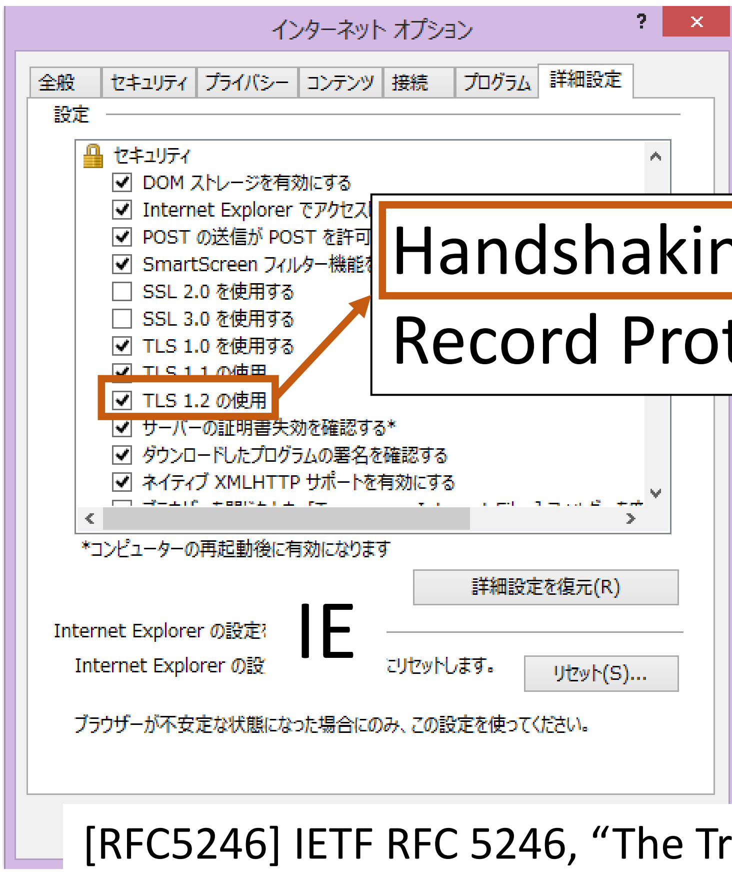
Advantages of Session Keys [Choo09]

- To limit the amount of cryptographic material
- To limit the exposure of messages
- To create independence
- To achieve efficiency

[Choo09] K.-K. R. Choo, “Secure Key Establishment,” Springer, 2009

AKE?!

- Widely used in practice



Handshaking Protocols

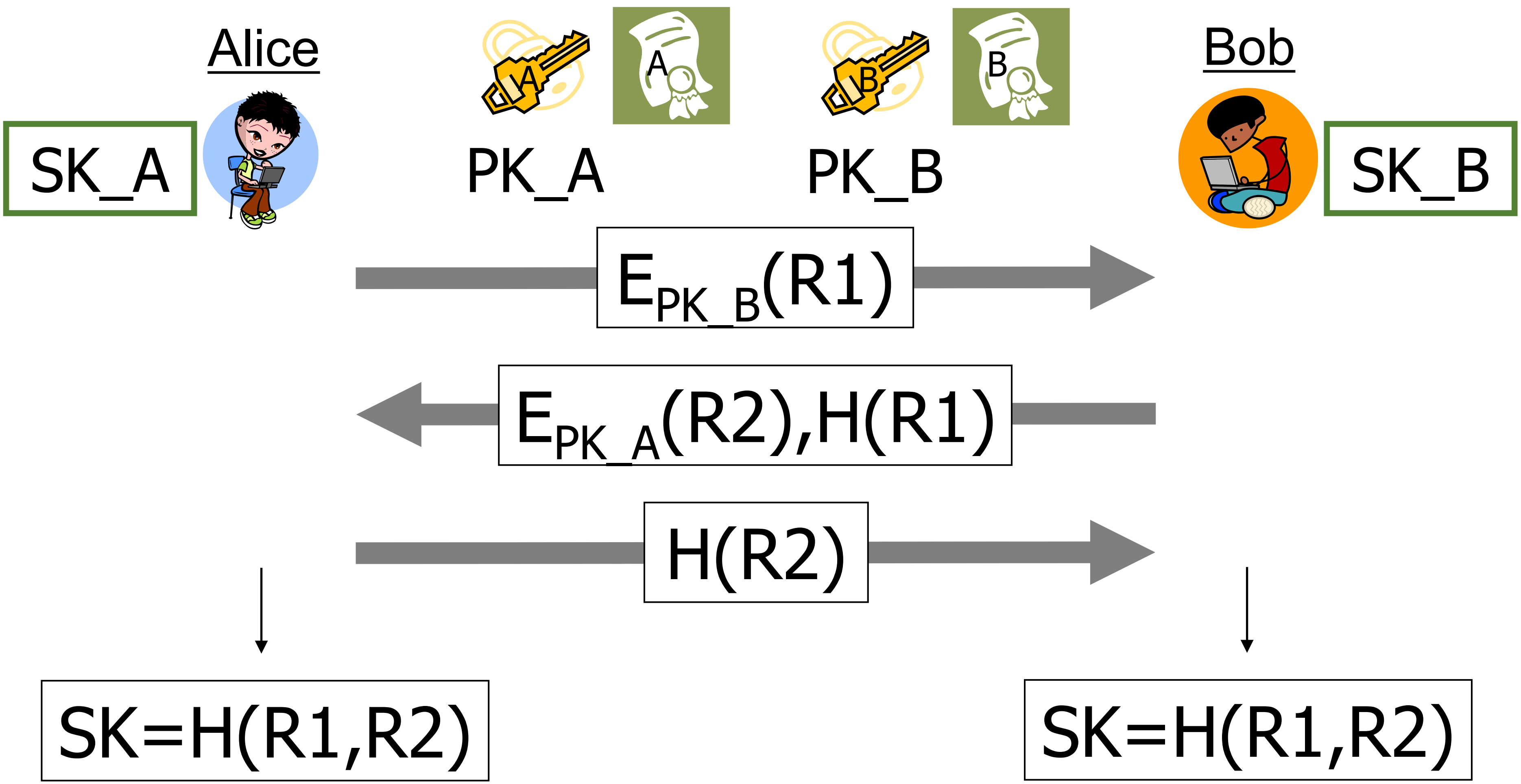
Record Protocol

Cipher Suites [RFC5246]

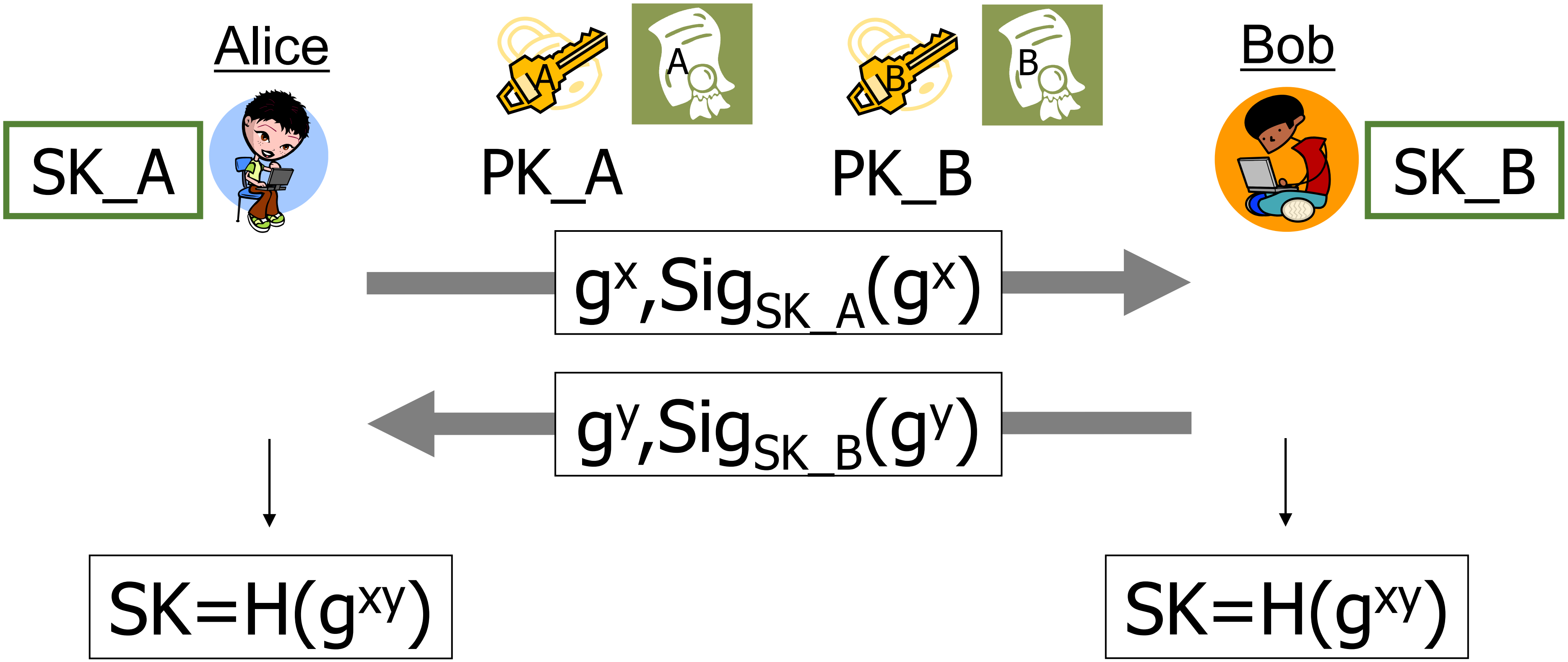
Cipher Suite	Key Exchange	Cipher	Mac
TLS_NULL_WITH_NULL_NULL	NULL	NULL	NULL
TLS_RSA_WITH_NULL_MD5	RSA	NULL	MD5
TLS_RSA_WITH_NULL_SHA	RSA	NULL	SHA
TLS_RSA_WITH_NULL_SHA256	RSA	NULL	SHA256
TLS_RSA_WITH_RC4_128_MD5	RSA	RC4_128	MD5
TLS_RSA_WITH_RC4_128_SHA	RSA	RC4_128	SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	3DES_EDE_CBC	SHA
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	AES_128_CBC	SHA
H_AES_256_CBC_SHA	RSA	AES_256_CBC	SHA
H_AES_128_CBC_SHA256	RSA	AES_128_CBC	SHA256
H_AES_256_CBC_SHA256	RSA	AES_256_CBC	SHA256
WITH_3DES_EDE_CBC_SHA	DH_DSS	3DES_EDE_CBC	SHA
WITH_3DES_EDE_CBC_SHA	DH_RSA	3DES_EDE_CBC	SHA
_WITH_3DES_EDE_CBC_SHA	DHE_DSS	3DES_EDE_CBC	SHA
_WITH_3DES_EDE_CBC_SHA	DHE_RSA	3DES_EDE_CBC	SHA
_WITH_RC4_128_MD5	DH_anon	RC4_128	MD5
_WITH_3DES_EDE_CBC_SHA	DH_anon	3DES_EDE_CBC	SHA
TLS_DH_DSS_WITH_AES_128_CBC_SHA	DH_DSS	AES_128_CBC	SHA
TLS_DH_RSA_WITH_AES_128_CBC_SHA	DH_RSA	AES_128_CBC	SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	DHE_DSS	AES_128_CBC	SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE_RSA	AES_128_CBC	SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA	DH_anon	AES_128_CBC	SHA
TLS_DH_DSS_WITH_AES_256_CBC_SHA	DH_DSS	AES_256_CBC	SHA
TLS_DH_RSA_WITH_AES_256_CBC_SHA	DH_RSA	AES_256_CBC	SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	DHE_DSS	AES_256_CBC	SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE_RSA	AES_256_CBC	SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA	DH_anon	AES_256_CBC	SHA
TLS_DH_DSS_WITH_AES_128_CBC_SHA256	DH_DSS	AES_128_CBC	SHA256
TLS_DH_RSA_WITH_AES_128_CBC_SHA256	DH_RSA	AES_128_CBC	SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	DHE_DSS	AES_128_CBC	SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE_RSA	AES_128_CBC	SHA256
TLS_DH_anon_WITH_AES_128_CBC_SHA256	DH_anon	AES_128_CBC	SHA256
TLS_DH_DSS_WITH_AES_256_CBC_SHA256	DH_DSS	AES_256_CBC	SHA256
TLS_DH_RSA_WITH_AES_256_CBC_SHA256	DH_RSA	AES_256_CBC	SHA256
			IA256
			IA256
			IA256

[RFC5246] IETF RFC 5246, “The Transport Layer Security (TLS) Protocol Version 1.2,” 2008

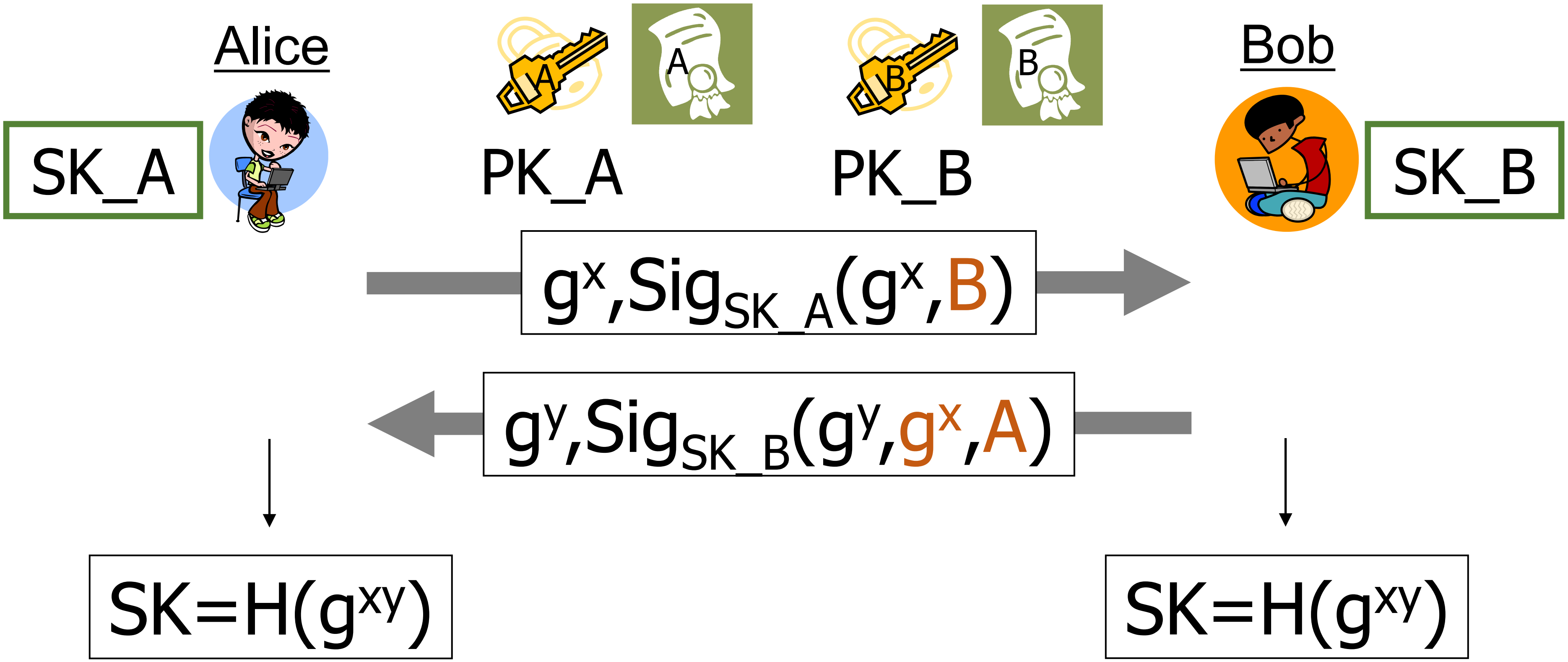
PKI based AKE



PKI based AKE

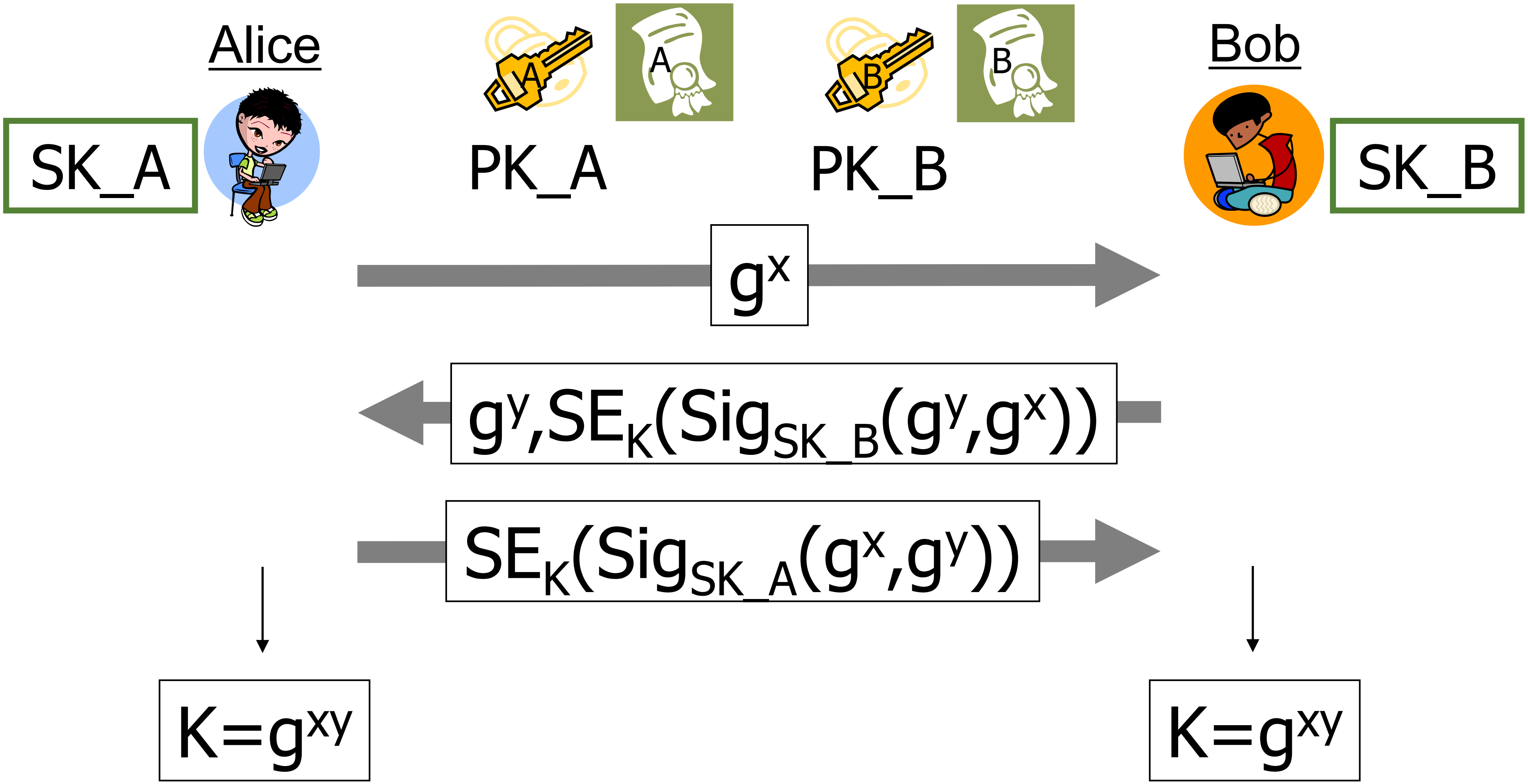


A Variant [Sho99, ISO/IEC9798-3]

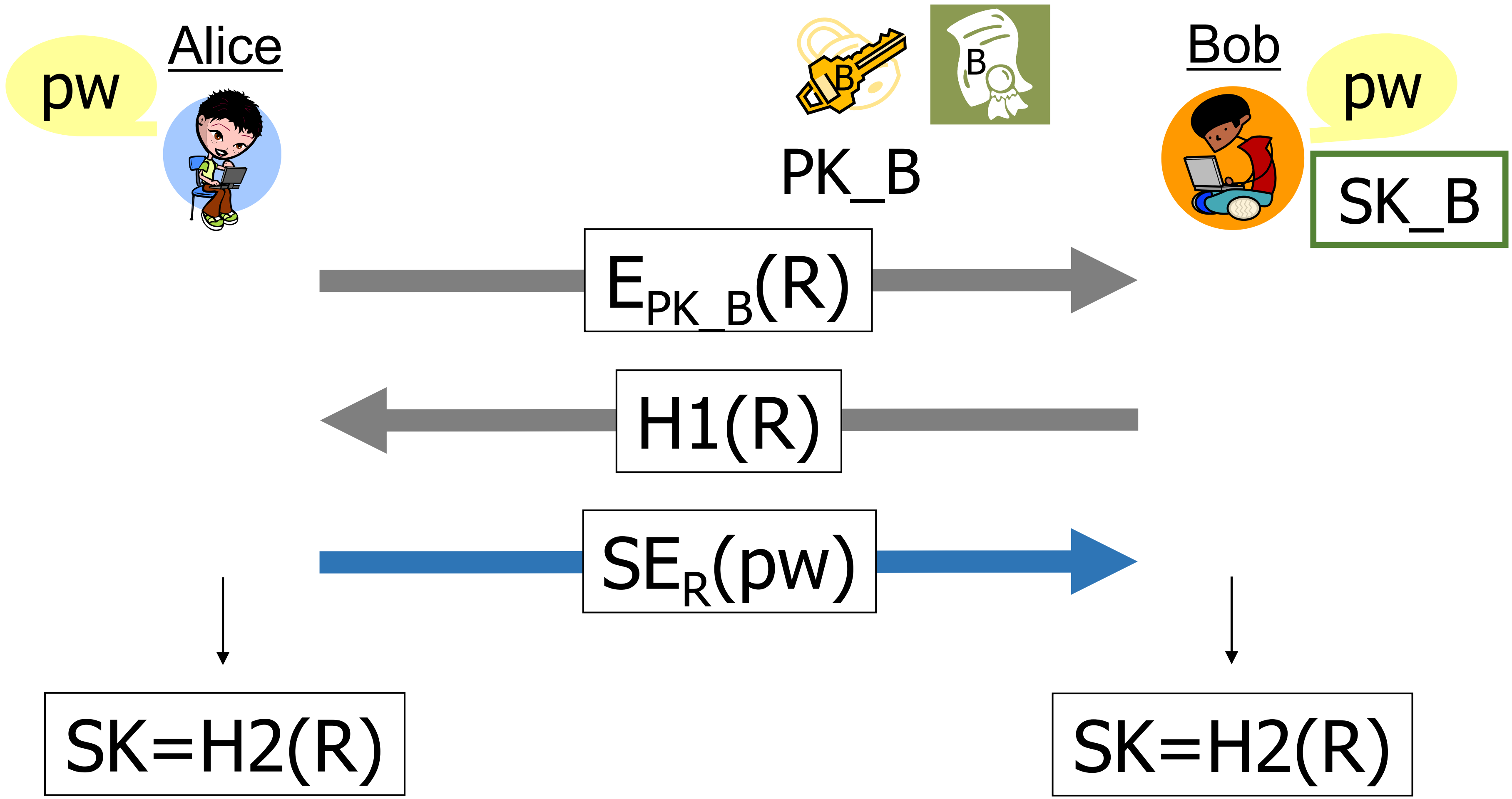


[Sho99] V. Shoup, “On Formal Models for Secure Key Exchange,” 1999
[ISO/IEC9798-3] ISO/IEC 9798-3, “IT Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques,” 2019

STS [DOW92]


Alice
Bob
SK_A
PK_A
PK_B
SK_B
A
B
g^x
$g^y, SE_K(Sig_{SK\_B}(g^y, g^x))$
$SE_K(Sig_{SK\_A}(g^x, g^y))$
$K=g^{xy}$
$K=g^{xy}$

PKI based AKE

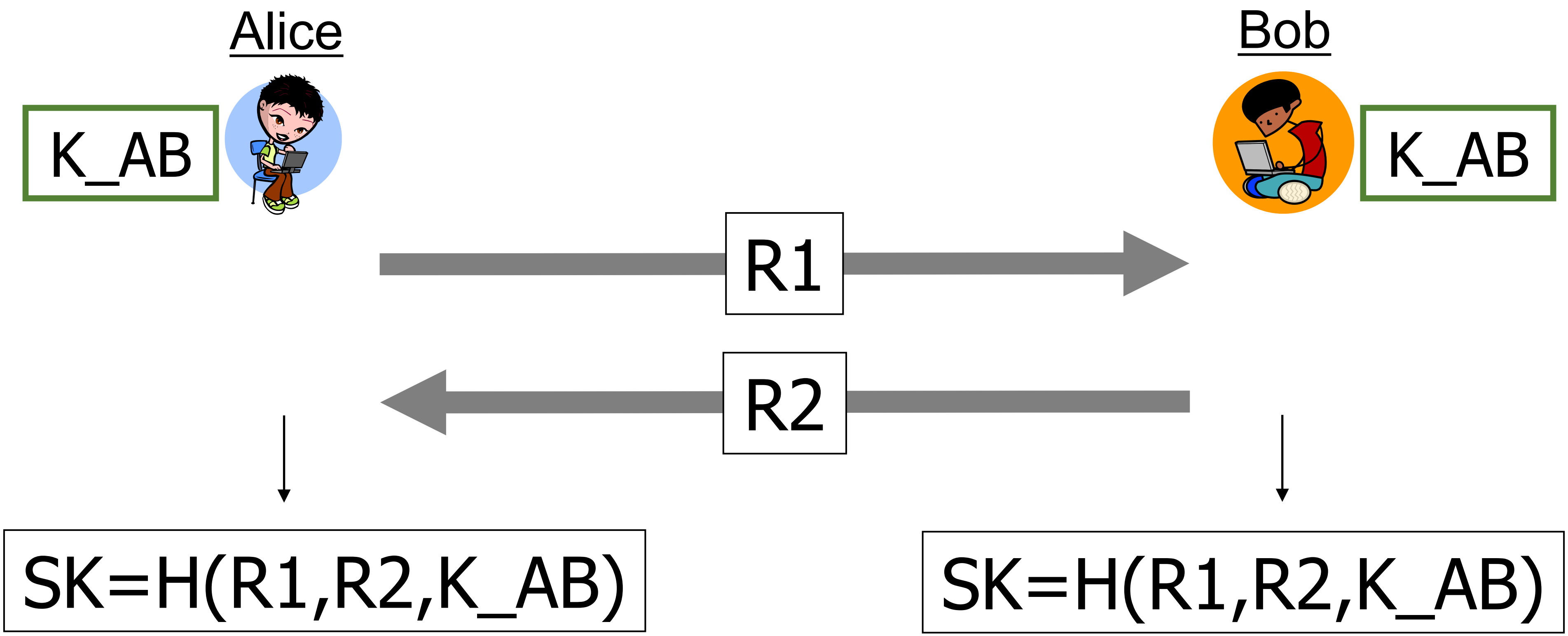


PKI

- Management of public keys
  - Certified by CA

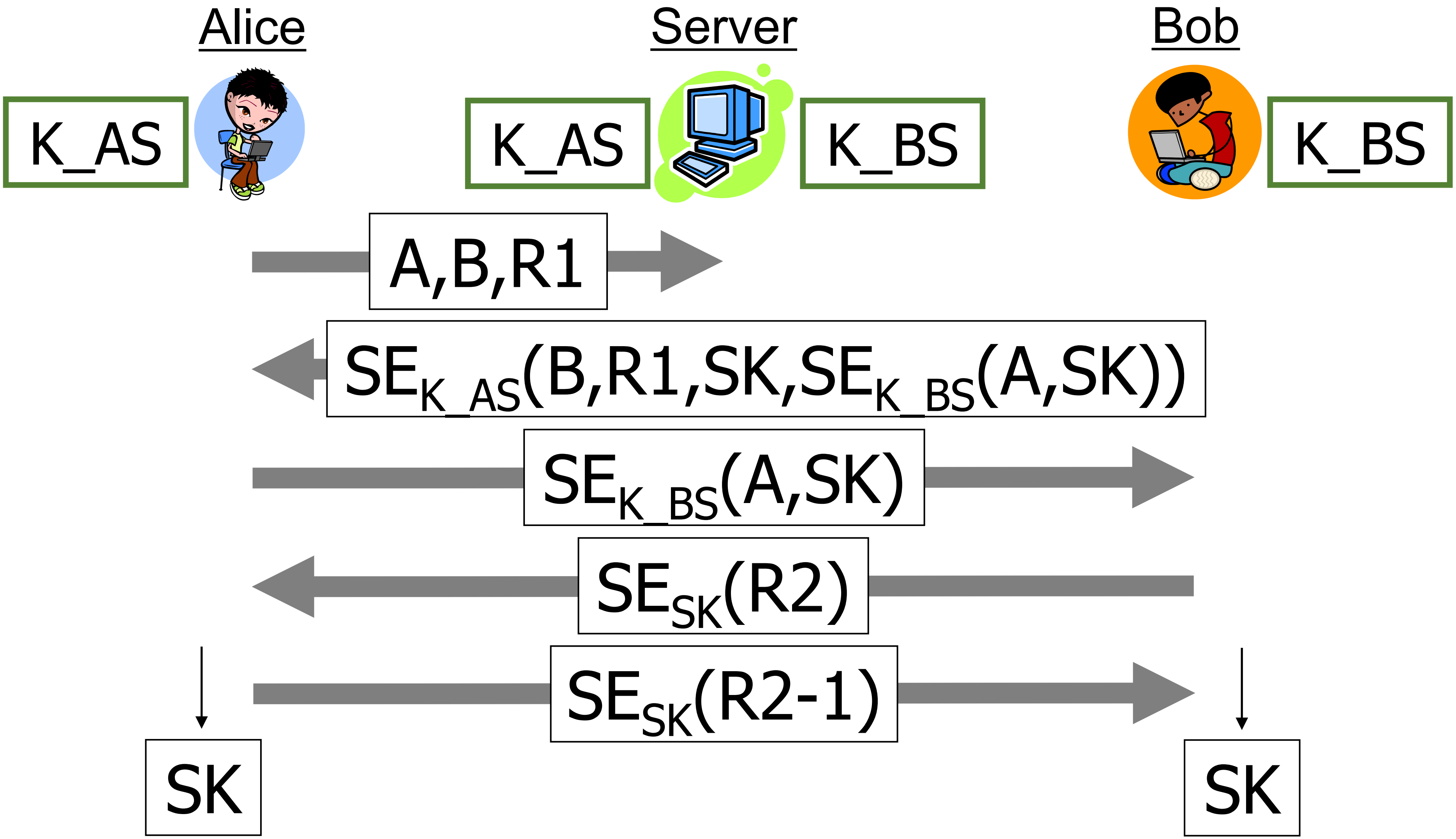
- In PKI based AKE protocols,
  - A party should **check the validity of** the counterpart's **public-key certificate** through CRL/OCSP/SCVP
  - E.g., Phishing attacks (social engineering attacks)

Two-Pass [Boyd95]



[Boyd95] C. Boyd, “Towards a Classification of Key Agreement Protocols,” 8th IEEE Computer Security Foundations Workshop, 1995

Needham-Schroeder [NS78]



Needham-Schroeder

- Insecure against
  - Known session key attack
  - Compromise of Alice's long-term key

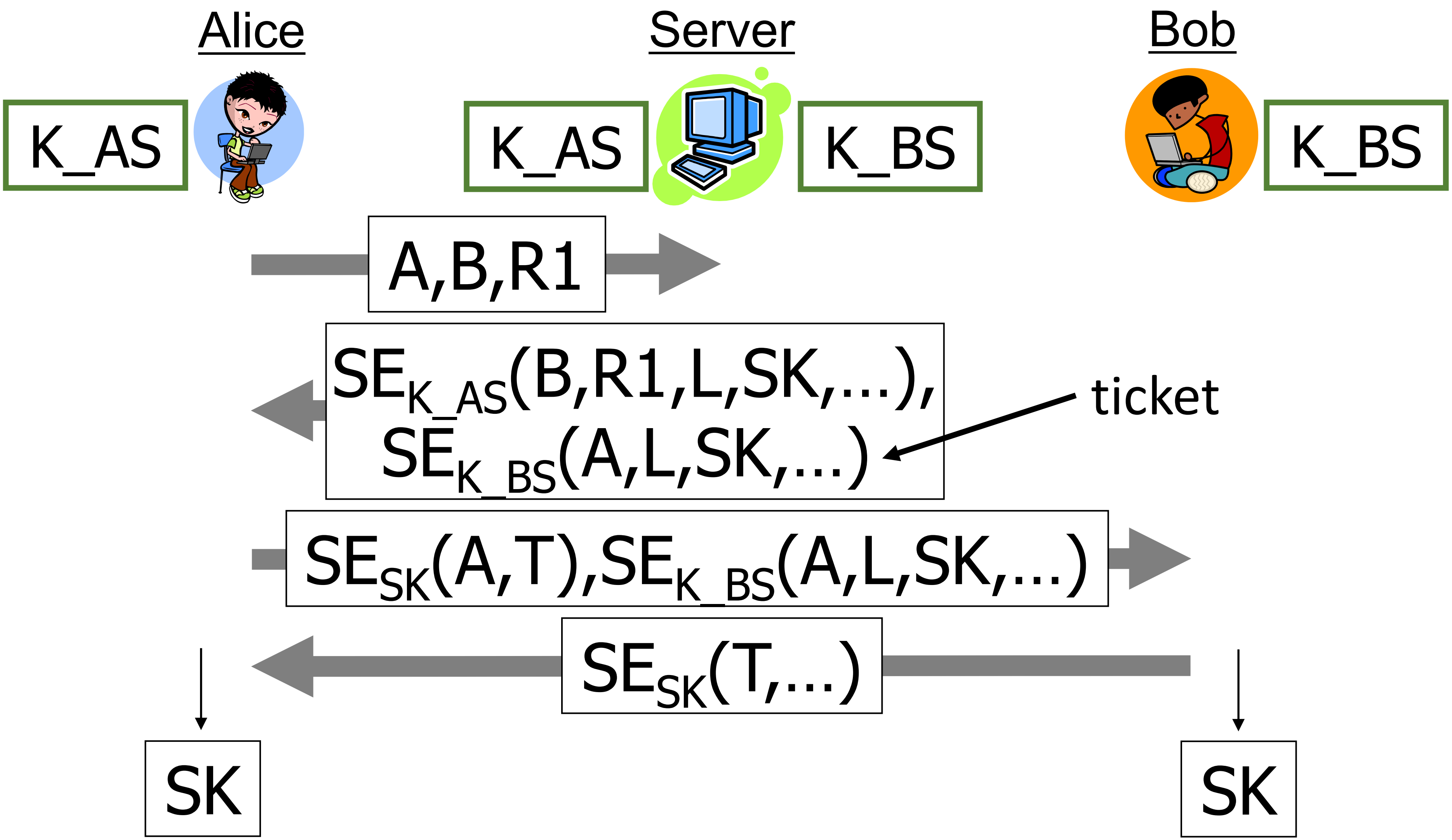
[NS78] R. M. Needham and M. D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers," Communications of the ACM, 1978

Kerberos [NT94, RFC4120]

- Building block
  - Needham-Schroeder [NS78]
  - With timestamps instead of nonces
- Version 5
  - Three parties: client, application server, authentication server

[NT94] B. C. Neuman and T. Ts'o, "Kerberos: an Authentication Service for Computer Networks," IEEE Communications Magazine, 1994
[RFC4120] IETF RFC 4120, "The Kerberos Network Authentication Service (V5)," 2005

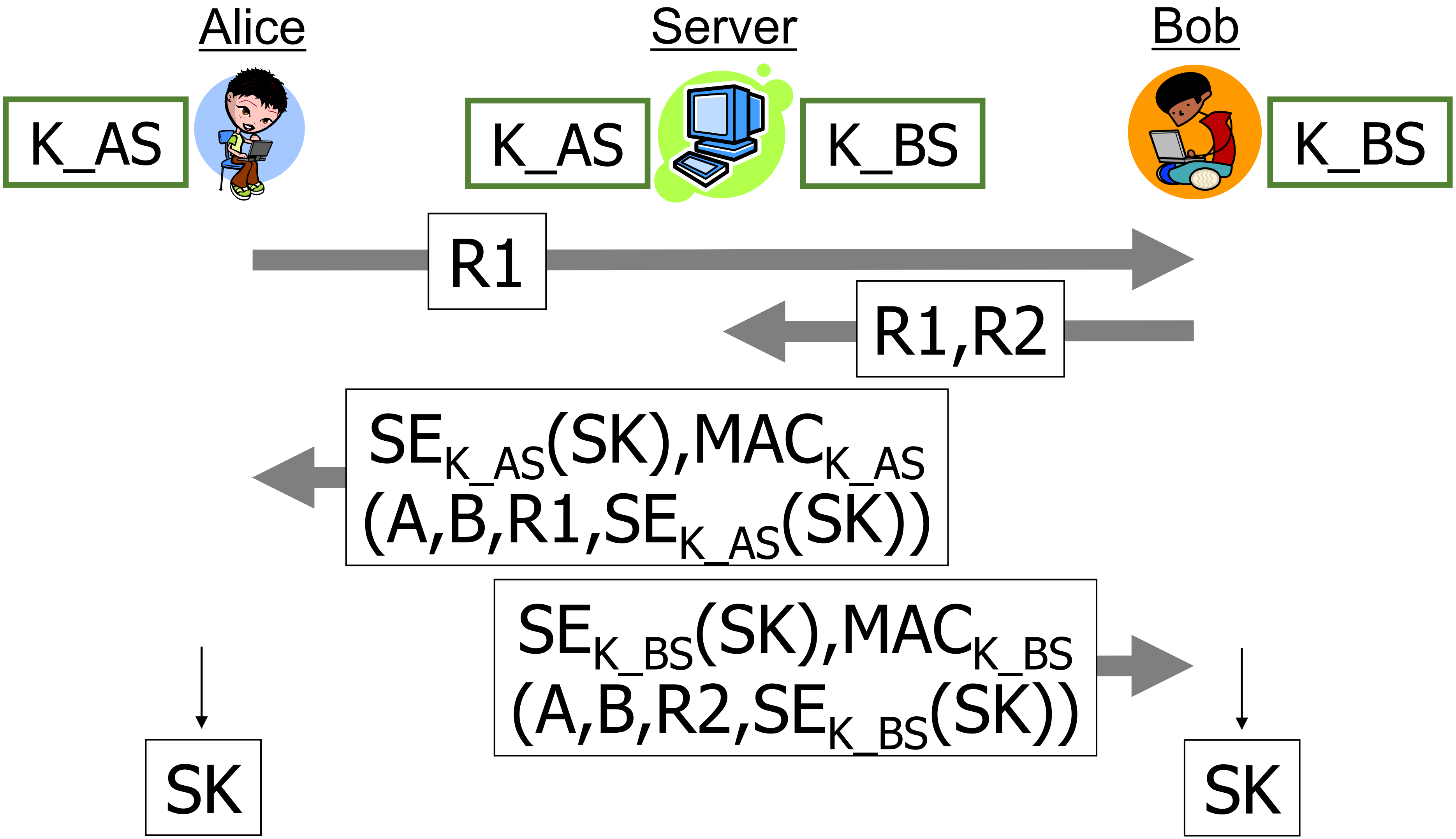
Kerberos


Alice
Server
Bob
K_AS
K_AS
K_BS
K_BS
A,B,R1
$SE_{K\_AS}(B,R1,L,SK,\ldots)$,
$SE_{K\_BS}(A,L,SK,\ldots)$
ticket
$SE_{SK}(A,T),SE_{K\_BS}(A,L,SK,\ldots)$
$SE_{SK}(T,\ldots)$
SK
SK

3PKD [BR95]

- Two different keys for SE and MAC
- Provably secure

3PKD

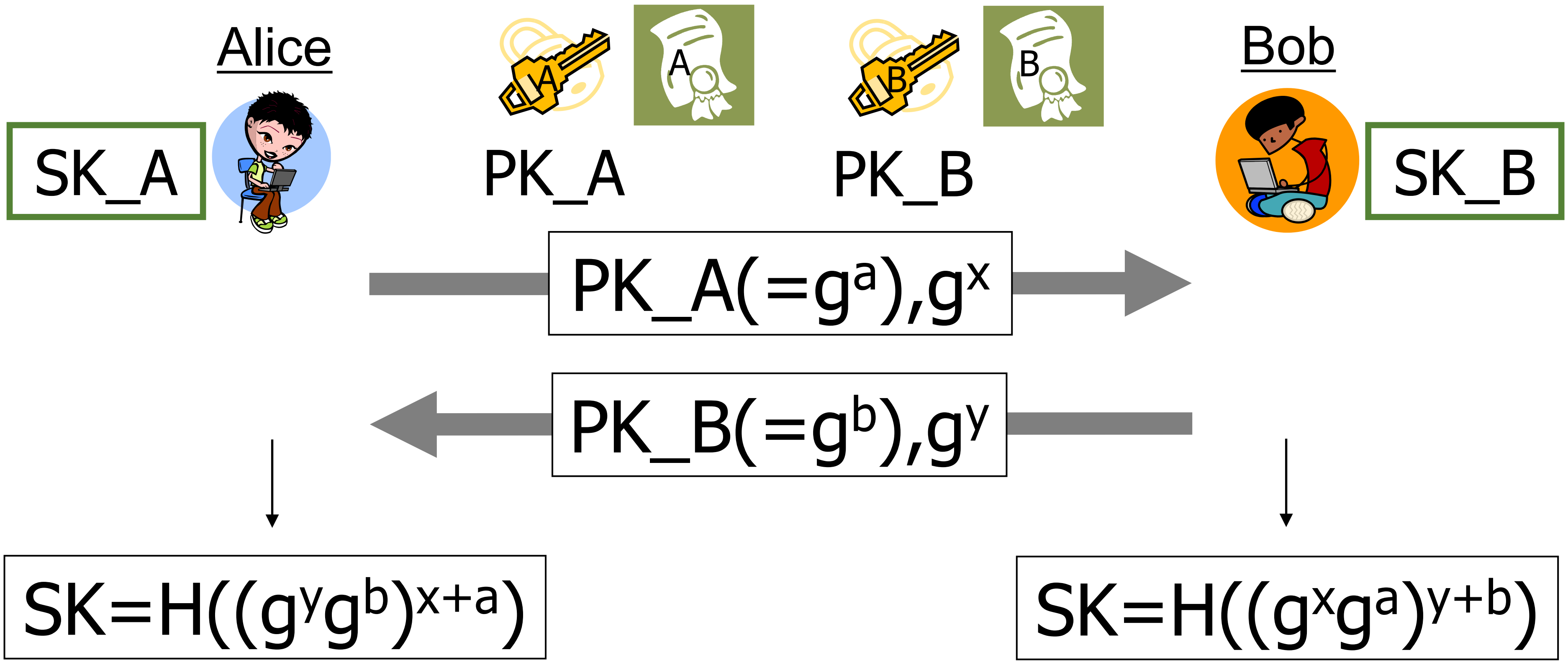

Alice
Server
Bob
K_AS
K_AS
K_BS
K_BS
R1
R1,R2
SE$_{K_AS}$(SK),MAC$_{K_AS}$(A,B,R1,SE$_{K_AS}$(SK))
SE$_{K_BS}$(SK),MAC$_{K_BS}$(A,B,R2,SE$_{K_BS}$(SK))
SK
SK

Unified Model [BJM97, X9.42, X9.63, IEEE1363]

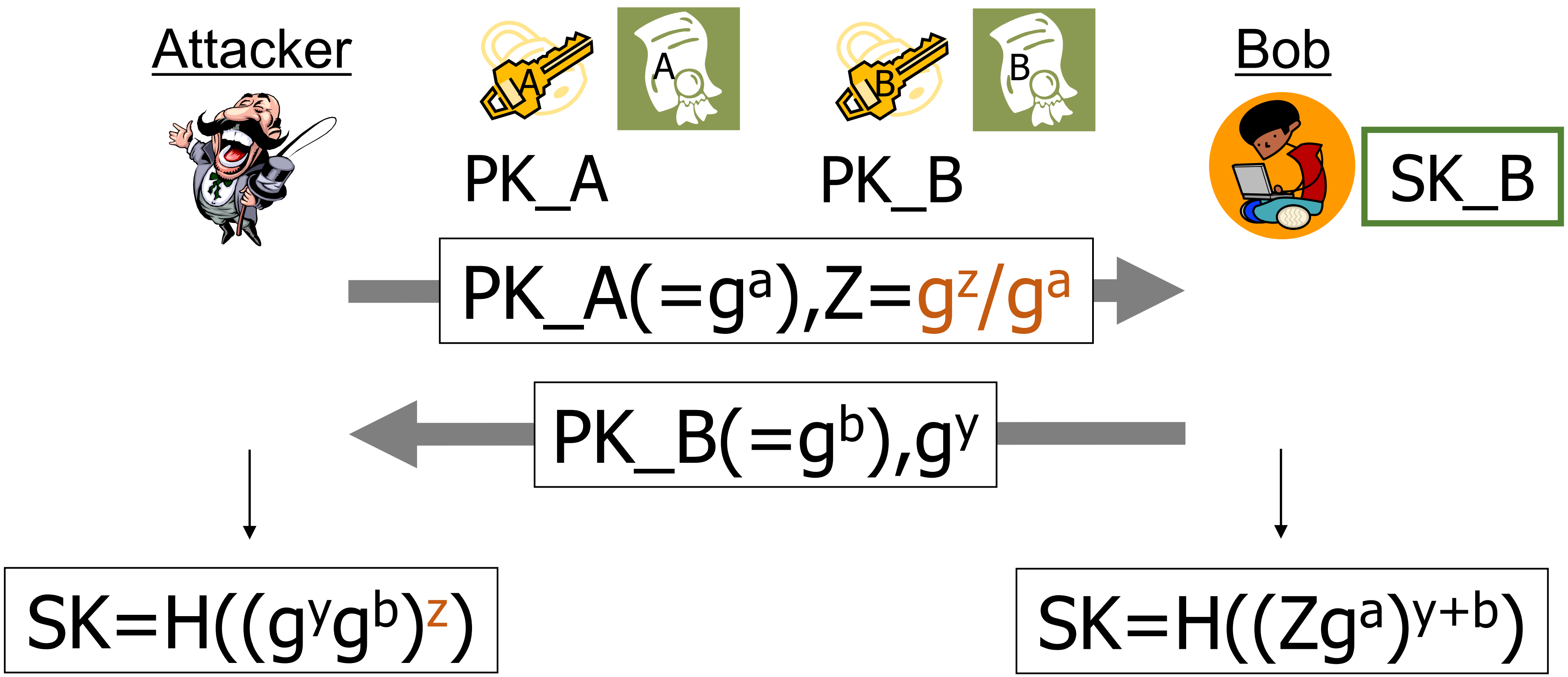
- Protocol abstraction
  - Both parties use their public keys to generate a shared key for authenticating the DH protocol
- Key compromise impersonation attack

[BJM97] S. Blake-Wilson, D. Johnson, and A. Menezes, “Key Agreement Protocols and their Security Analysis,” IMA International Conference on Cryptography and Coding, 1997
[X9.42] ANSI X9.42, “Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography,” 2003
[X9.63] ANSI X9.63, “Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography,” 2011
[IEEE1363] IEEE 1363, “IEEE Standard Specifications for Public-Key Cryptography,” 2000

Is it secure?

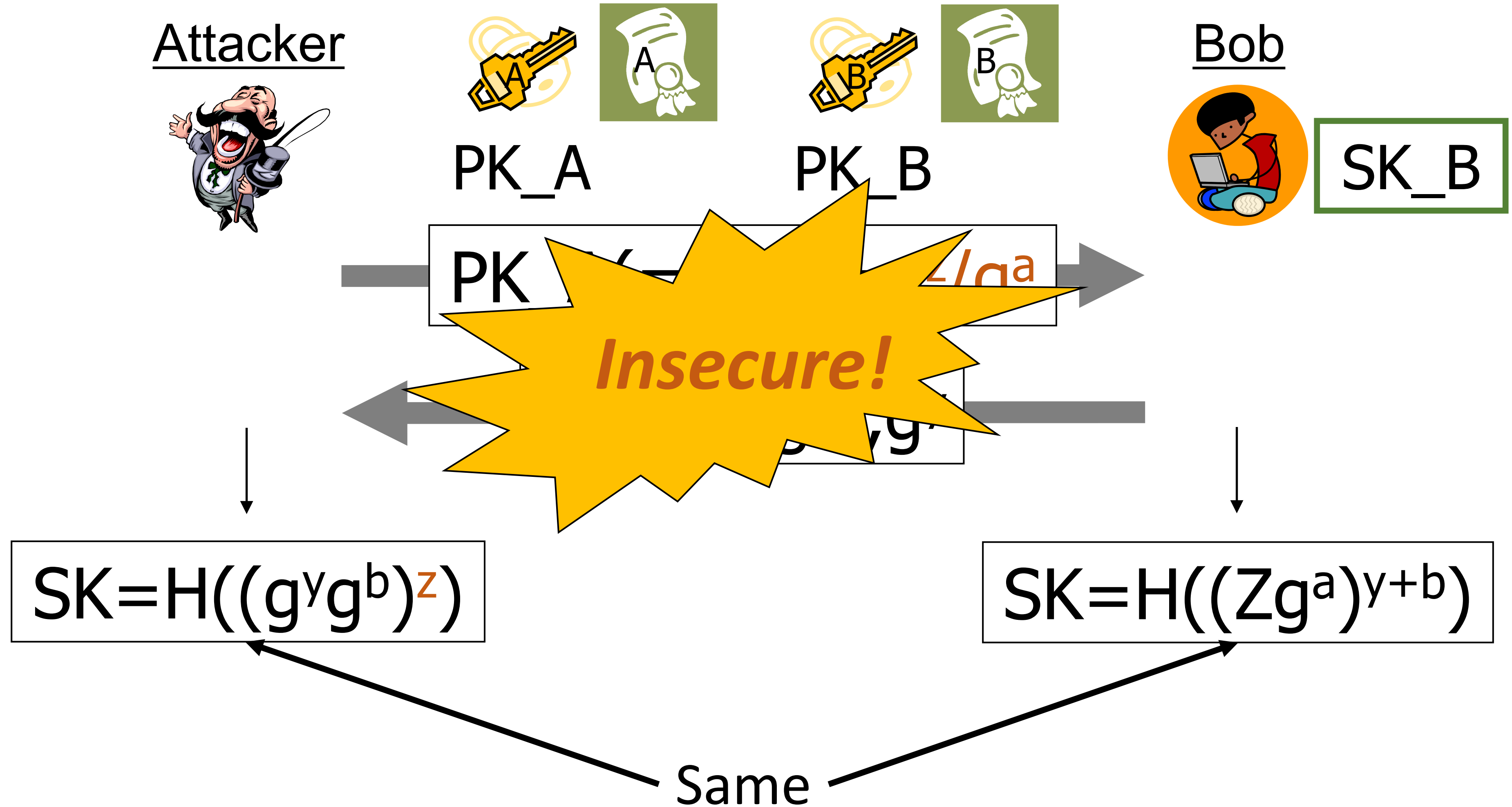

Alice
SK_A
A
PK_A
B
PK_B
Bob
SK_B
$PK\_A(=g^a),g^x$
$PK\_B(=g^b),g^y$
$SK=H((g^y g^b)^{x+a})$
$SK=H((g^x g^a)^{y+b})$

“No”



Attacker
A
A
PK_A
B
B
PK_B
Bob
SK_B
PK_A(=g^a),Z=g^z/g^a
PK_B(=g^b),g^y
SK=H((g^y g^b)^z)
SK=H((Zg^a)^(y+b))

“No”



MQV [MQV95, LMQ+03, X9.42, X9.63, IEEE1363, ISO/IEC11770-3, NIST800-56A]

- "Implicitly-authenticated"
  - Initiated by [MTI86]
- **Most efficient**

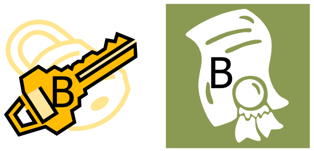
[MTI86] T. Matsumoto, Y. Takashima, and H. Imai, "On Seeking Smart Public-Key-Distribution Systems," IEICE Transactions, 1986
[MQV95] A. J. Menezes, M. Qu, and S. A. Vanstone, "Some New Key Agreement Protocols Providing Implicit Authentication," SAC'95
[LMQ+03] L. Law et. al., "An Efficient Protocol for Authenticated Key Agreement," Designs, Codes and Cryptography, 2003
[ISO/IEC11770-3] ISO/IEC 11770-3, "Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques," 2015
[NIST800-56A] NIST SP 800-56A, "Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography," 2018

MQV

Alice

SK_A

PK_A



PK_B

Bob

SK_B

PK_A(=g^a),g^x →

← PK_B(=g^b),g^y

$SK=H((g^y g^{be})^{x+ad})$

$SK=H((g^x g^{ad})^{y+be})$

$e=2^l+(g^y \bmod 2^l)$, $d=2^l+(g^x \bmod 2^l)$, and $l=|q|/2$

MQV

- (Online) unknown-key share attack
- Leakage of “session-specific information,” not considered

HMQV [Kra05]

- Hashed MQV

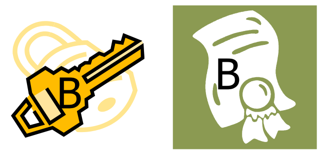
[Kra05] H. Krawczyk, “HMQV: A High-Performance Secure Diffie-Hellman Protocol,” CRYPTO 2005

HMQV

Alice

SK_A

PK_A



PK_B

Bob

SK_B

$PK\_A(=g^{a}),g^{x}$ →

← $PK\_B(=g^{b}),g^{y}$

$SK=H((g^{y}g^{be})^{x+ad})$

$SK=H((g^{x}g^{ad})^{y+be})$

$e=H1(g^{y},A),\ d=H1(g^{x},B)$

Password based AKE

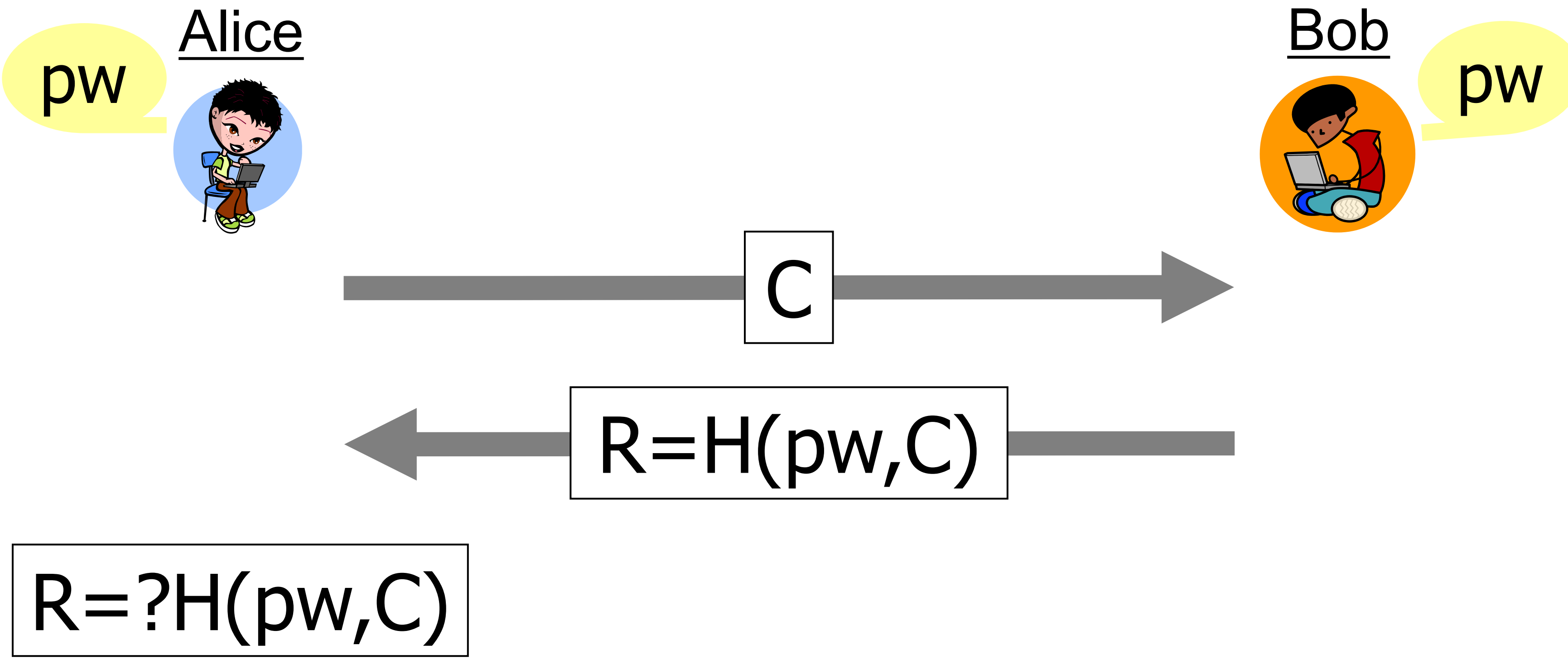
Passwords (Weak Secrets)

- Hereafter, assuming that **PKI is not available**
- Passwords are chosen from a small set of dictionary
  - Practical usability
  - 4-digit PIN codes
  - Alphanumerical passwords with 6 characters
  - Exhaustive search is possible

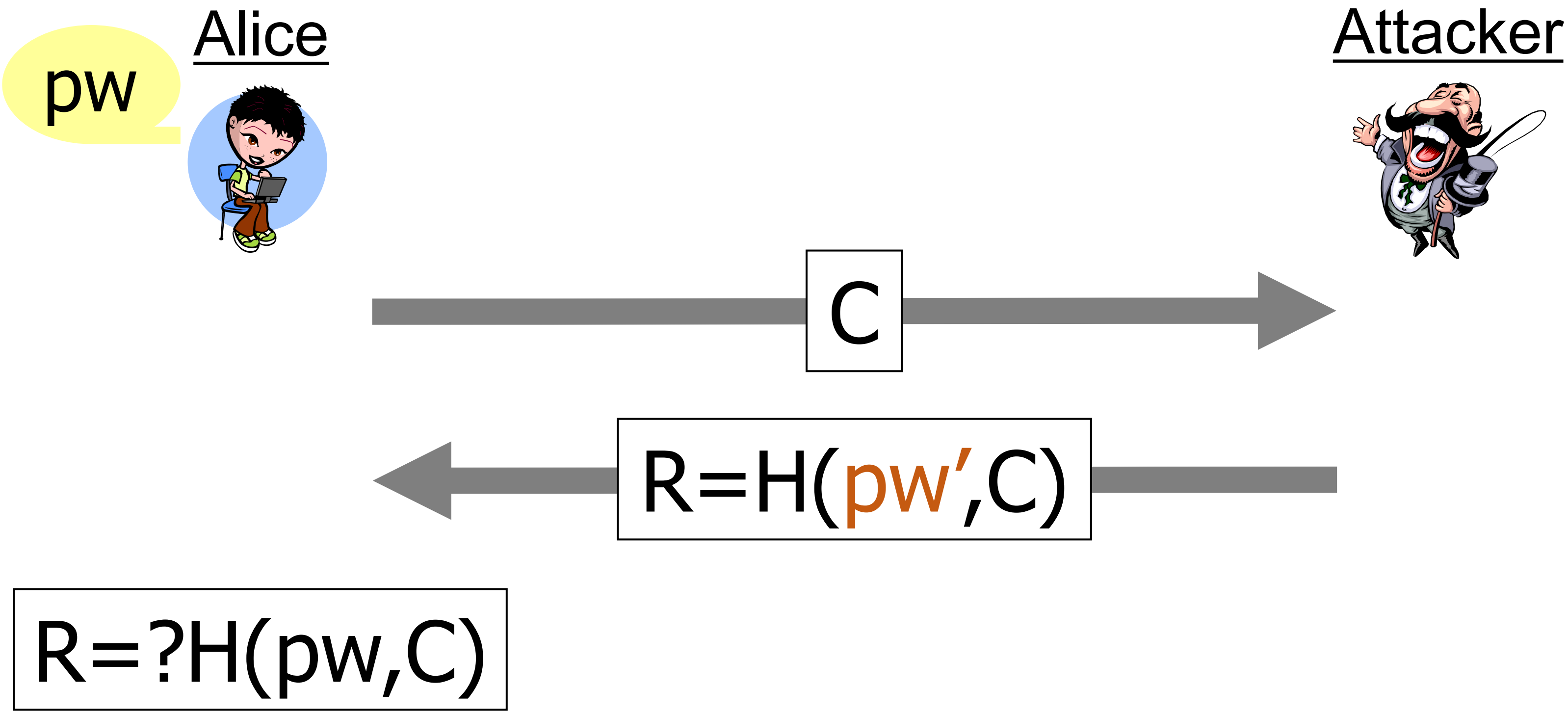
Password dictionary

gertrude	holly	joy	lara	marietta	neptune	patty
gibson	homework	joyce	larkin	mark	ness	paula
gina	honey	judith	larry	markus	net	pencil
ginger	horse	judy	laura	marni	network	penelope
glacier	horus	juggle	lazarus	mars	new	penguin
gnu	hutchins	julia	leah	marty	news	penis
golf	hydrogen	julie	lebesgue	marvin	newton	peoria
golfer	ibm	june	lee	mary	next	percolate
gorgeous	imbroglio	jupiter	leland	master	nicole	persimmon
gorges	imperial	karen	leroy	math	nita	persona
gosling	include	karie	leslie	maurice	nobody	pete
gouge	ingres	karina	lewis	meagan	noreen	peter
graham	ingress	kate	library	megan	noxious	philip
grahm	ingrid	kathleen	light	melissa	nuclear	phoenix
group	inna	kathrine	linda	mellon	nutrition	phone
gryphon	innocuous	kathy	lisa	memory	nyquist	pierre
gucci	internet	katina	lisp	mercury	oceanograph	pizza
guess	irene	katrina	liz	merlin	y	plane
guest	irishman	kelly	lock	mets	ocelot	playboy
guitar	isis	keri	lockout	mgr	office	plover
gumption	jackie	kermit	lois	michael	olivetti	pluto
guntis	jane	kernel	lori	michele	olivia	plymouth
hack	janet	kerri	lorin	michelle	open	polly
hacker	janice	kerrie	lorraine	mickey	operator	polynomial
hal	janie	kerry	louis	mike	oracle	pondering
hamlet	japan	key	love	minimum	orca	pork
handily	jasmin	kim	lucy	minsky	orwell	porsche
happening	jean	kimberly	lynn	mit	osiris	poster
harmony	jeanne	kirkland	lynne	modem	outlaw	power
harold	jen	kitten	macintosh	mogul	oxford	praise
harvey	jenni	knight	mack	moguls	pacific	precious
hawaii	jennifer	krista	maggot	monica	pad	prelude
heather	jenny	kristen	magic	moose	painless	presto
hebrides	jessica	kristi	mail	morley	pakistan	prince
heidi	jester	kristie	maint	mouse	pam	princeton
heinlein	jill	kristin	malcolm	mozart	pamela	priv
hello	jixian	kristine	malcom	mutant	paper	private
help	joanne	kristy	manager	nagel	papers	privs
herbert	jody	ladle	mara	nancy	pass	professor
hiawatha	johnny	lambda	marci	napoleon	password	profile
hibernia	joseph	lamination	marcy	nasa	pat	program
hidden	joshua	lana	maria	nepenthe	patricia	protect

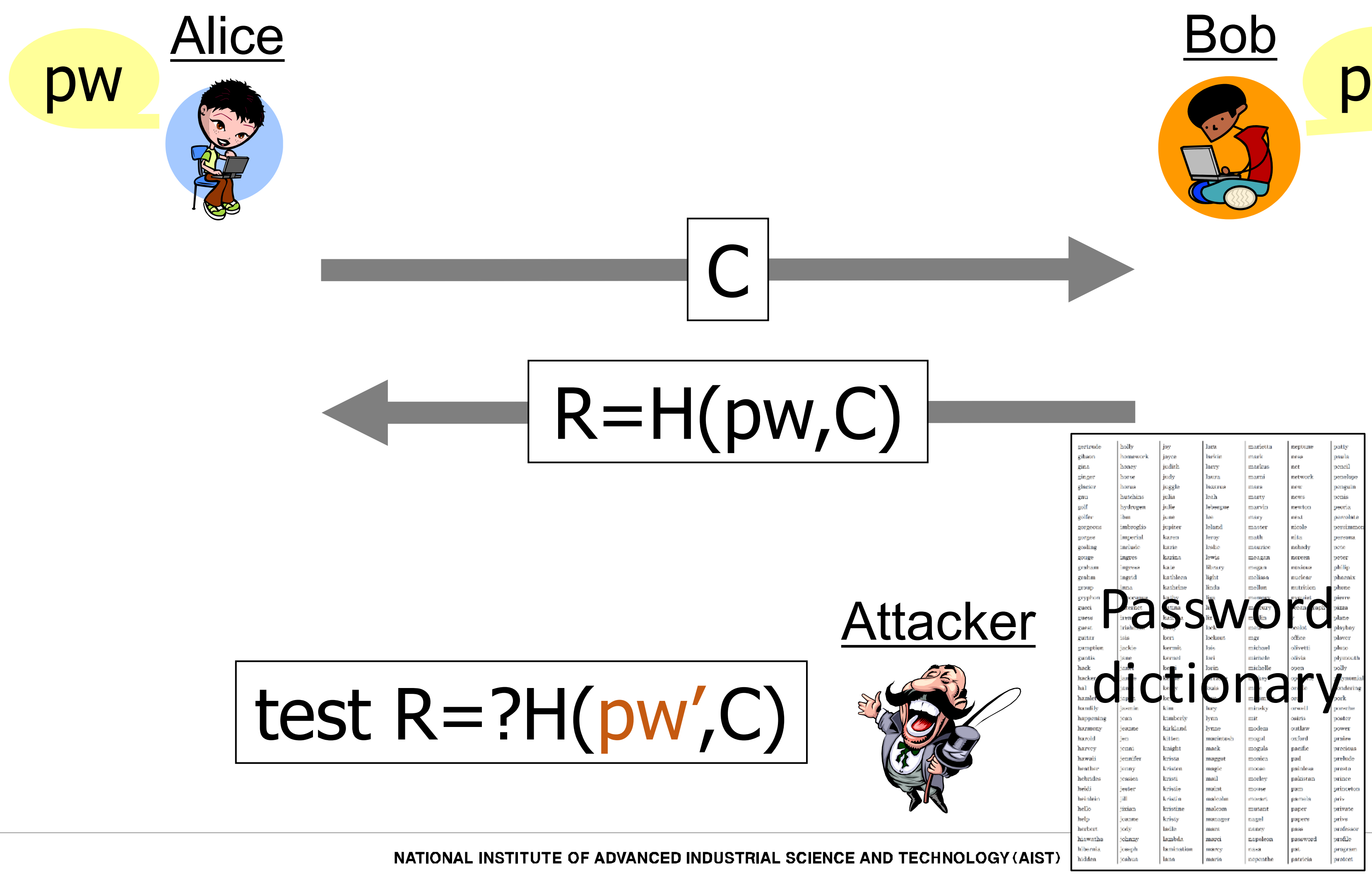
Password based Authentication



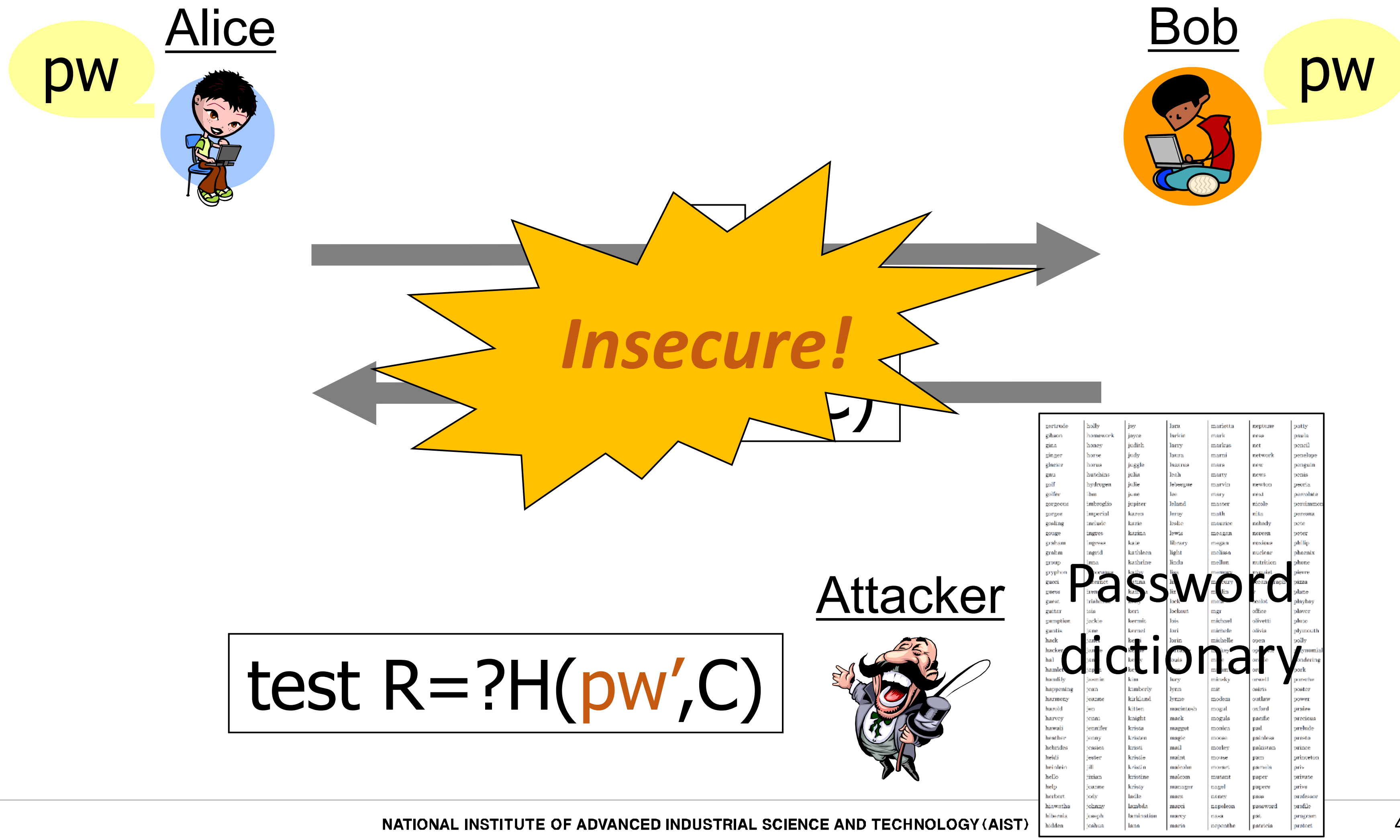
Online Dictionary Attacks



Offline Dictionary Attacks



Offline Dictionary Attacks



Estimated Password Guessing Entropy in bits vs. Password Length [NIST800-63]

	User Chosen				Randomly Chosen	
	94 Character Alphabet			10 char. alphabet		94 char alphabet
Length Char.	No Checks	Dictionary Rule	Dict. & Comp. Rule			
1	4	-	-	3	3.3	6.6
2	6	-	-	5	6.7	13.2
3	8	-	-	7	10.0	19.8
4	10	14	16	9	13.3	26.3
5	12	17	20	10	16.7	32.9
6	14	20	23	11	20.0	39.5
7	16	22	27	12	23.3	46.1
8	18	24	30	13	26.6	52.7
10	21	26	32	15	33.3	65.9
12	24	28	34	17	40.0	79.0
14	27	30	36	19	46.6	92.2
16	30	32	38	21	53.3	105.4
18	33	34	40	23	59.9	118.5
20	36	36	42	25	66.6	131.7
22	38	38	44	27	73.3	144.7
24	40	40	46	29	79.9	158.0
30	46	46	52	35	99.9	197.2
40	56	56	62	45	133.2	263.4

[NIST800-63] NIST SP 800-63, "Electronic Authentication Guideline," 2006

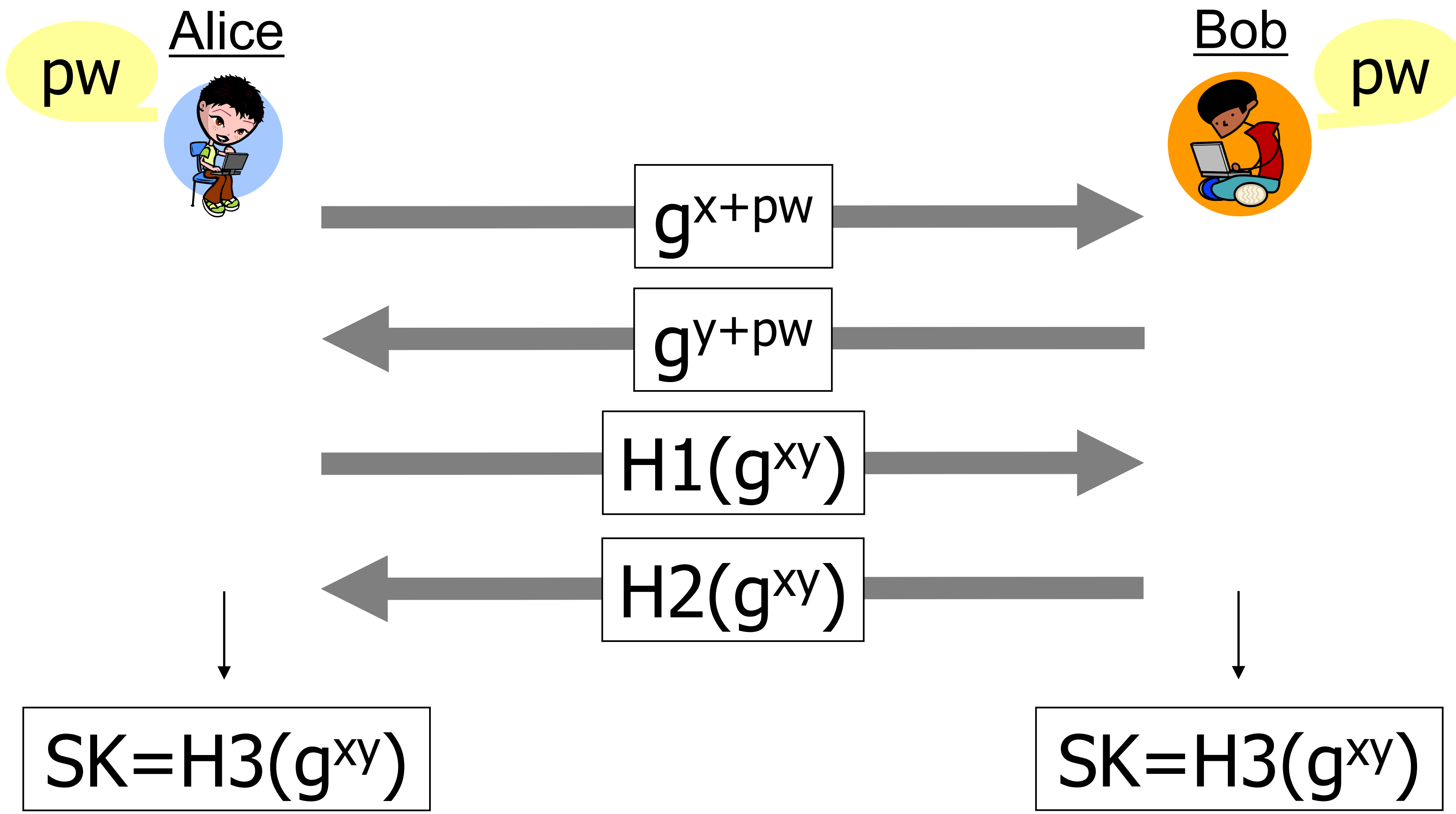
Security Goal

- Two exhaustive search attacks
  - Online dictionary attacks can be easily prevented by taking appropriate countermeasures
  - **Offline dictionary attacks should be avoided**
- Security goal
  - Secure against passive/active attacks
  - Prevent an attacker from performing offline dictionary attacks

Password based AKE

- Not trivial
  - **Some redundancy can be used** in offline dictionary attacks
  - **No clear guideline** to avoid offline dictionary attacks
  - Need to **bootstrap a weak secret to a strong one**
  - …

Is it secure?



"No"

pw

Alice

Attacker

$M1=g^{x+pw}$ →

← $g^{y+pw'}$

$R1=H1(K)$ →

$K=(g^{y+pw'-pw})^{x}$

"No"

pw

<u>Alice</u>

<u>Attacker</u>

Alice → Attacker: $M1=g^{x+pw}$

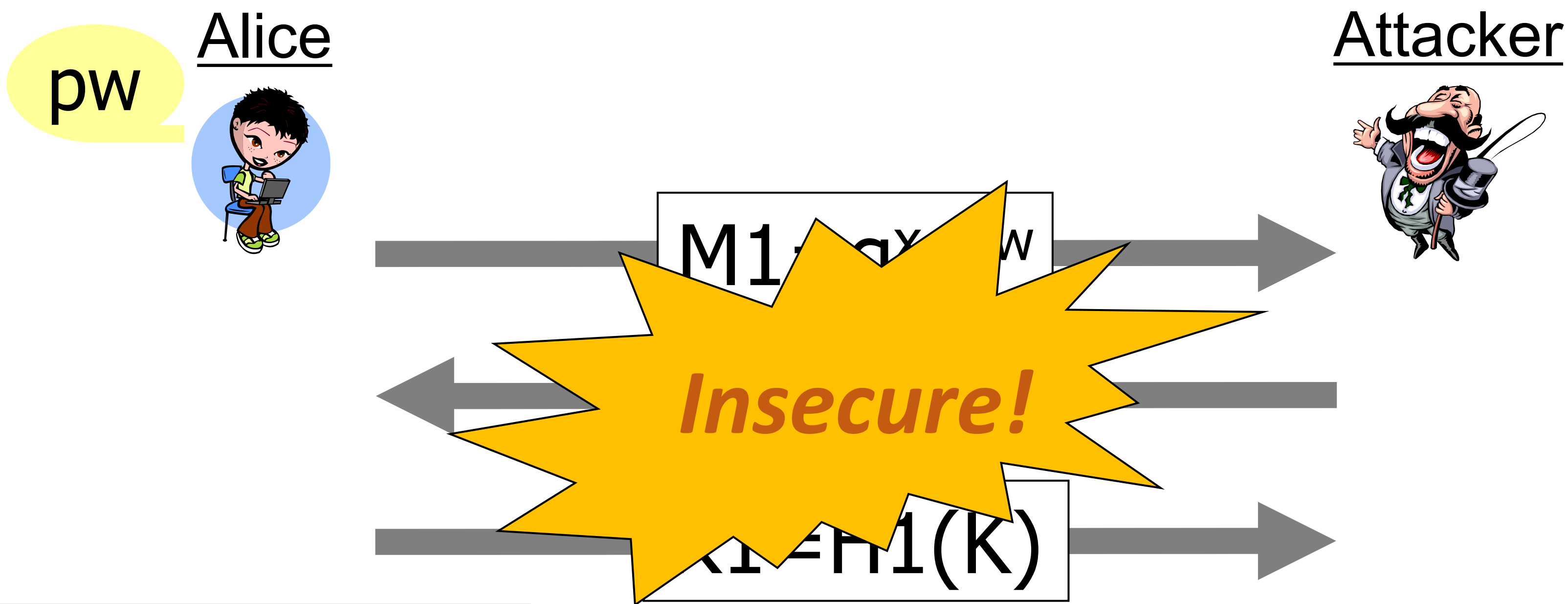
Attacker → Alice: $g^{y+pw'}$

Alice → Attacker: $R1=H1(K)$

$K=(g^{y+pw'-pw})^{x}$

$$K=(g^{y+pw'-pw})^{x}$$
$$=(g^{x})^{y+pw'-pw}$$
$$=(M1/g^{pw})^{y+pw'-pw}$$

"No"



$K=(g^{y+pw'-pw})^x$

$K=(g^{y+pw'-pw})^x$

$=(g^x)^{y+pw'-pw}$

$=(M1/g^{pw})^{y+pw'-pw}$

Password-Authenticated Key Exchange

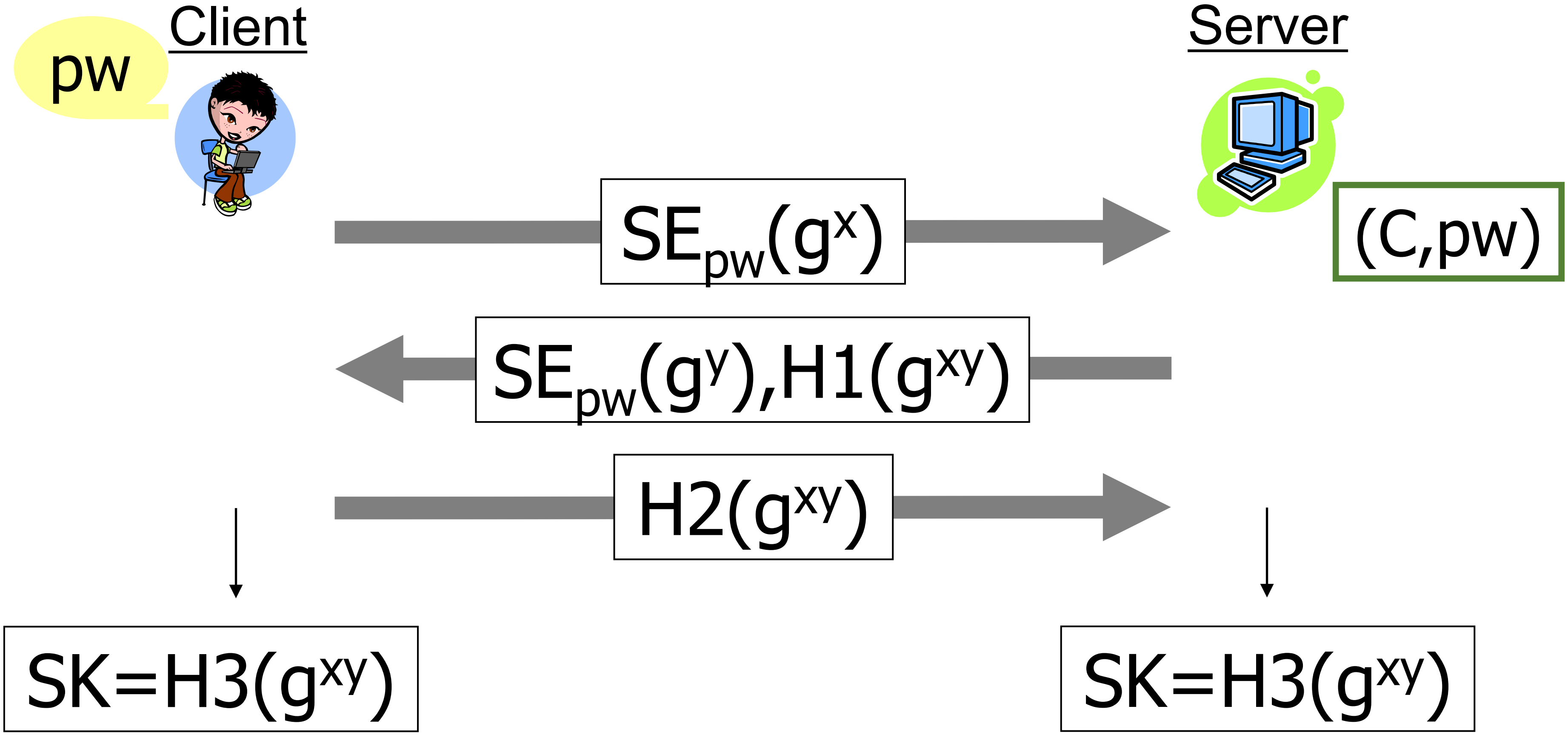
Password-Authenticated Key Exchange (PAKE)

- Password-only setting

- Some ideas for secure PAKE
  - **A combination of symmetric and asymmetric cryptographic techniques** [BM92]
  - From other cryptographic primitives (e.g., OT)

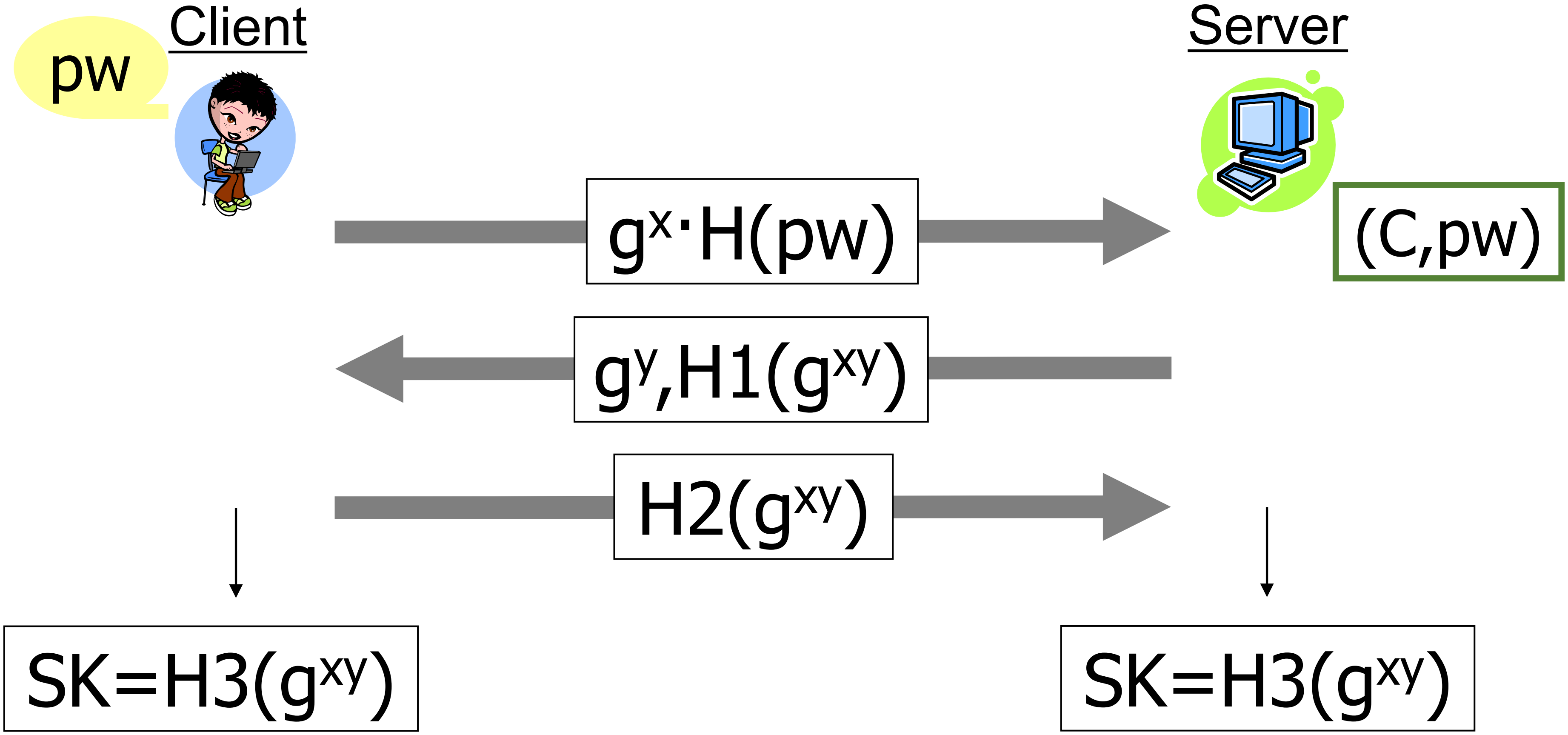
[BM92] S. M. Bellovin and M. Merritt, “Encrypted Key Exchange: Password-based Protocols Secure against Dictionary Attacks,” IEEE Symposium on Security and Privacy, 1992

Secure PAKE [BPR00]



[BPR00] M. Bellare, D. Pointcheval, and P. Rogaway, “Authenticated Key Exchange Secure against Dictionary Attacks,” EUROCRYPT 2000

Secure PAKE [BCP04]



[BCP04] E. Bresson, O. Chevassut, and D. Pointcheval, “New Security Results on Encrypted Key Exchange,” PKC 2004

Secure PAKE [KI02]

Client

pw

Server

(C,pw)

Client → Server: $g^x \cdot h^{pw}$

Server → Client: $g^y \cdot h^{pw}$

Client → Server: $H1(g^{xy})$

Server → Client: $H2(g^{xy})$

Client: $SK=H3(g^{xy})$

Server: $SK=H3(g^{xy})$

[KI02] K. Kobara and H. Imai, "Pretty-Simple Password-Authenticated Key-Exchange Protocol Proven to be Secure in the Standard Model," IEICE Transactions, 2002

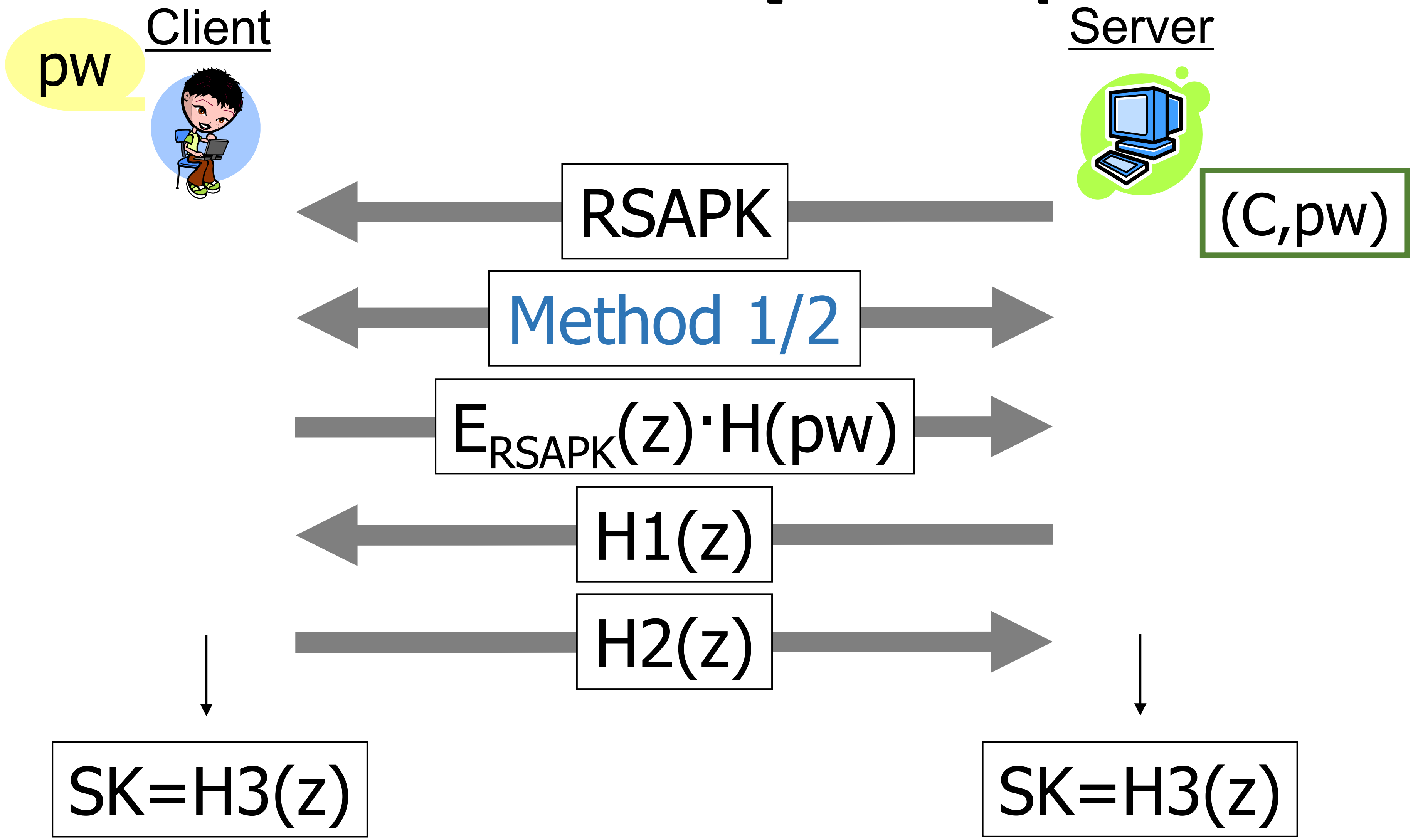
Secure PAKE [**S**KI08a]

- Two challenge/response methods for RSAPK
  - **Method 1**: using RSA encryption
  - **Method 2**: using RSA signature

- **Any odd prime e**

[**S**KI08a] **S. H. Shin**, K. Kobara, and H. Imai, "RSA-Based Password-Authenticated Key-Exchange, Revisited," IEICE Transactions, 2008

Secure PAKE [SKI08a]



ISO/IEC 11770-4:2017 [ISO/IEC11770-4]

- Balanced Key Agreement Mechanism
  - BKAM1 [Jab96]
  - BKAM2 [HR08]

[ISO/IEC11770-4] ISO/IEC 11770-4, “Information technology – Security techniques – Key management – Part 4: Mechanisms based on weak secrets,” Second edition, 2017
[Jab96] D. Jablon, “Strong Password-Only Authenticated Key Exchange,” Computer Communication Review, 1996
[HR08] F. Hao and P. Ryan, “Password Authenticated Key Exchange by Juggling,” 16th Workshop on Security Protocols, 2008

ISO/IEC 11770-4:2017 [ISO/IEC11770-4]

- Augmented Key Agreement Mechanism
  - AKAM1 [Wu02]
  - AKAM2 [Kwon00, Kwon03]
  - AKAM3 [**S**K12]

[Wu02] T. Wu, "SRP-6: Improvements and Refinements to the Secure Remote Password Protocol," 2002
[Kwon00] T. Kwon, "Ultimate Solution to Authentication via Memorable Password," 2000
[Kwon03] T. Kwon, "Addendum to Summary of AMP," 2003
[**S**K12] **S. H. Shin** and K. Kobara, "Efficient Augmented Password-Only Authentication and Key Exchange for IKEv2," IETF RFC 6628, 2012

IEEE 1363.2-2008 [IEEE1363.2]

- Password-authenticated key agreement schemes
  - BPKAS-PAK
  - BPKAS-PPK
  - BPKAS-SPEKE
  - APKAS-AMP
  - APKAS-BSPEKE2
  - APKAS-PAKZ
  - (DL) APKAS-SRP3, APKAS-SRP6
  - (EC) APKAS-SRP5
  - APKAS-WSPEKE

[IEEE1363.2] IEEE 1363.2, “IEEE Standard Specifications for Password-Based Public-Key Cryptographic Techniques,” 2008

Augmented PAKE

- Inherent limitations of PAKE
  - **Online dictionary attacks** are always possible
  - Sever compromise always leads to **password exposure**
  - **No client anonymity**

- Balanced PAKE
  - Server compromise allows direct client impersonation
- Augmented PAKE
  - **Extra protection for server compromise** (i.e., resistance to server compromise impersonation attack)

Augmented PAKE

- A-EKE, AuthA, VB-EKE
- B-SPEKE
- PAK-X/Y/Z/Z+

- SRP [IEEE1363.2, ISO/IEC11770-4, RFC2945, RFC5054]
- AMP [IEEE1363.2, ISO/IEC11770-4]

[RFC2945] IETF RFC 2945, “The SRP Authentication and Key Exchange System,” 2000
[RFC5054] IETF RFC 5054, “Using the Secure Remote Password (SRP) Protocol for TLS Authentication,” 2007

AugPAKE [**S**K12, ISO/IEC11770-4]

- Efficiency
  - **Most efficient**
  - Similar computational efficiency to plain DH key exchange
- Security
  - Secure against passive/active attacks
  - Secure against offline dictionary attacks
  - Resistance to server compromise impersonation attacks

AugPAKE

Client C (w) — **Server S ($W=g^w$)**

Client: $X=g^x$

$\xrightarrow{\quad C,\ X \quad}$

Server: $K=g^y$

$r=H(1|C|S|X)$

$Y=(X\cdot W^r)^y$

$\xleftarrow{\quad S,\ Y \quad}$

Client: $r=H(1|C|S|X)$

$z=1/(x+w\cdot r) \bmod q$

$K=Y^z$

$\xrightarrow{\quad V\_C=H(2|C|S|X|Y|K) \quad}$

$\xleftarrow{\quad V\_S=H(3|C|S|X|Y|K) \quad}$

Client: $SK=H(4|C|S|X|Y|K)$

Server: $SK=H(4|C|S|X|Y|K)$

Comparison

- Computation costs

*SRP should use a safe prime

Protocols	Number of modular exp. (excluding pre-computable costs)	
	Client C	Server S
DH key exchange	2 (1)	2 (1)
AugPAKE	**2** (**1**)	**2.17** (**1.17**)
SRP	3 (2)	**2.17*** (**1.17***)
AMP	**2** (**1**)	2.34 (2.34)

- Communication costs of SRP, AMP and AugPAKE
  - 2 group elements + 2 hash values

Features of AugPAKE

- **Security and efficiency** (as before)
- **Any cryptographically secure DH groups** can be used
  - Neither FDH nor IC used
- **Forward secrecy**
- Can be easily **converted to ‘balanced’ one**

Performance Overhead

- For better efficiency and security

- AugPAKE over EC groups and with domain parameters [**S**KI15]

[**S**KI15] **S. H. Shin**, K. Kobara, and H. Imai, "On Finding Secure Domain Parameters Resistant to Cheon's Algorithm," IEICE Transactions, 2015

Processing Time of AugPAKE Client on Raspberry Pi 2

unit (ms)

Domain parameters [15]	Average	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th	11th	12th	13th	14th	15th
SECp160r1	172.3	175	169	173	174	183	159	168	166	173	173	162	194	174	173	169
SECp192r1	176.6	177	186	173	183	195	178	170	172	164	178	174	174	175	172	178
SECp224r1	219.0	224	230	221	210	219	217	217	220	221	225	217	222	213	228	201
SECp256r1	187.0	183	201	181	188	183	208	188	179	187	176	186	184	196	180	185
SECp384r1	201.9	207	222	202	220	210	198	217	188	197	186	191	187	196	207	201
SECp521r1	263.2	257	279	269	265	264	243	257	267	251	261	261	251	299	257	267
SECt163r2	186.5	180	194	184	182	190	189	181	177	214	179	193	177	187	191	180
SECt233r1	181.4	167	182	203	201	203	188	170	171	169	161	176	167	189	186	188
SECt283r1	213.5	200	206	219	201	221	193	207	208	207	221	207	272	207	229	204
SECt409r1	312.1	326	317	296	333	323	318	311	297	296	304	326	322	307	312	293
SECt571r1	527.1	558	534	504	525	537	527	519	559	519	493	515	552	522	523	519

- The bigger the domain parameter is, the longer the processing time of AugPAKE client is

Anonymous PAKE

Anonymous PAKE

- PAKE does **not** provide **client anonymity**

- Anonymous PAKE
  - Similar to group authentication
  - Honest-but-curious setting
  - **Anonymity against outsider/passive server**

  - APAKE, EAP, NAPAKE, VEAP, …

ISO/IEC 20009-4:2017 [ISO/IEC20009-4]

- Password-only PAEA mechanisms
  - SKI mechanism [**S**KI10a]
  - YZ mechanism [YZ08]
- Storage-extra PAEA mechanism
  - YZW mechanism [YZW+10]

[ISO/IEC20009-4] ISO/IEC 20009-4, "Information technology – Security techniques – Anonymous entity authentication – Part 4: Mechanisms based on weak secrets," 2017
[**S**KI10a] **S. H. Shin**, K. Kobara, and H. Imai, "Anonymous Password-Authenticated Key Exchange: New Construction and Its Extensions," IEICE Transactions, 2010
[YZ08] J. Yang and Z. Zhang, "A New Anonymous Password Based Authenticated Key Exchange Protocol," INDOCRYPT 2008
[YZW+10] Y. Yang, J. Zhou, J. W. Wong, and F. Bao, "Towards Practical Anonymous Password Authentication," ACSAC 2010

VEAP [**S**KI10a, ISO/IEC20009-4]

- Very-Efficient Anonymous PAKE (VEAP)
  - Based on blind signature scheme
  - **Provably secure**
    - AKE security
    - Anonymity against semi-honest server
  - **Most efficient**
    - With pre-computation
  - Its extensions

VEAP

User U_i (pw_i)

Server S $((U_j, pw_j),\ 1 \le j \le n)$

[Pre-computation]

$x \overset{R}{\leftarrow} \mathbb{Z}_p^\star$, $X \equiv g^x$, MS $\overset{R}{\leftarrow} \{0,1\}^l$

For $j = 1$ to n,

$W_j \leftarrow \mathcal{G}(U_j, pw_j)$,

$K_j \equiv (W_j)^x$, $\mathcal{K}_j \leftarrow \mathcal{F}(U_j, X, W_j, K_j)$,

and $C_j = \mathcal{E}_{\mathcal{K}_j}(\text{MS})$.

$W_i \cdot g^a$

$a \overset{R}{\leftarrow} \mathbb{Z}_p^\star$, $W_i \leftarrow \mathcal{G}(U_i, pw_i)$,

$A \equiv W_i \times g^a$

U, A →

Compute A^x

$V_S \leftarrow \mathcal{H}_1(U \| S \| \text{TRANS} \| \text{MS})$

A^x

← $S, X, A^x, \{C_j\}_{1 \le j \le n}, V_S$

$K_i \equiv A^x / X^a$

$\mathcal{K}_i \leftarrow \mathcal{F}(U_i, X, W_i, K_i)$,

For $i = j$, MS$' = \mathcal{D}_{\mathcal{K}_i}(C_i)$.

If V… $\|\text{TRANS}\|\text{MS}')$, reject.

Ot… $\leftarrow \mathcal{H}_2(U \| S \| \text{TRANS} \| \text{MS}')$

A^x/X^a

V_{U_i} →

$SK \leftarrow \mathcal{H}_3(U \| S \| \text{TRANS} \| \text{MS}')$

and accept.

If $V_{U_i} \ne \mathcal{H}_2(U \| S \| \text{TRANS} \| \text{MS})$, reject.

Otherwise, $SK \leftarrow \mathcal{H}_3(U \| S \| \text{TRANS} \| \text{MS})$

and accept.

Fig. 1 A very-efficient anonymous PAKE (VEAP) protocol where $\text{TRANS} = A \| A^x \| X \| \{C_j\}_{1 \le j \le n}$

Efficiency Comparison

- Computation/communication costs

Table 1 Efficiency comparison of anonymous PAKE protocols in terms of computation and communication costs where n is the number of users

Protocols	The number of modular exponentiations				Communication costs *1
	User U_i		Server S		
	Total	Total−Precomp.	Total	Total−Precomp.	
APAKE [24]	6	4	$4n+2$	$3n+1$	$(n+2)\|p\|+(n+1)\|\mathcal{H}\|$
TAP [21]	3	2	$n+1$	n	$2\|p\|+(n+1)\|\mathcal{H}\|$
NAPAKE [25]	4	3 *2	$n+3$	2	$(n+3)\|p\|+\|\mathcal{H}\|$ *2
VEAP	2	1	$n+2$	1	$3\|p\|+2\|\mathcal{H}\|+n\|\mathcal{E}\|$

*1: The bit-length of identities is excluded

*2: In [25], they incorrectly estimated the efficiency of the NAPAKE protocol. Note that $\mathcal{G}:\{0,1\}^* \to \mathbb{G}^*$

Same costs as DH key exchange

AIST

Extension 1: Communication Costs

Server S $((U_j, pw_j),\ 1 \le j \le n)$

[Publication of temporarily-fixed values]

$x \xleftarrow{R} \mathbb{Z}_p^\star, X \equiv g^x, \mathsf{MS} \xleftarrow{R} \{0,1\}^l$

For $j = 1$ to n,

$W_j \leftarrow \mathcal{G}(U_j, pw_j)$,

$K_j \equiv (W_j)^x, \mathcal{K}_j \leftarrow \mathcal{F}(U_j, X, W_j, K_j)$,

and $C_j = \mathcal{E}_{\mathcal{K}_j}(\mathsf{MS})$.

Server S's public bulletin board			
Posted time	Users U	Values	Valid period t
2009/01/18	$\{U_j\}_{1 \le j \le n}$	$X, \{C_j\}_{1 \le j \le n}$	up to 2009/02/17

read

[Protocol execution up to t]

$x, X, (\mathcal{K}_j, C_j),\ 1 \le j \le n$

User U_i (pw_i)

$(a, b) \xleftarrow{R} (\mathbb{Z}_p^\star)^2,\ B \equiv g^b$,

$W_i \leftarrow \mathcal{G}(U_i, pw_i),\ A \equiv W_i \times g^a$

U, A, B →

$y \xleftarrow{R} \mathbb{Z}_p^\star,\ Y \equiv g^y$

Compute A^x, B^x and B^y

$V_S \leftarrow \mathcal{H}_1(U \| S \| \textsc{trans} \| B^x \| B^y \| \mathsf{MS})$

← S, A^x, Y, V_S

$K_i \equiv A^x / X^a$,

$\mathcal{K}_i \leftarrow \mathcal{F}(U_i, X, W_i, K_i)$,

For $i = j$, $\mathsf{MS}' = \mathcal{D}_{\mathcal{K}_i}(C_i)$.

If $V_S \ne \mathcal{H}_1(U \| S \| \textsc{trans} \| X^b \| Y^b \| \mathsf{MS}')$, reject.

Otherwise, $V_{U_i} \leftarrow \mathcal{H}_2(U \| S \| \textsc{trans} \| X^b \| Y^b \| \mathsf{MS}')$

$SK \leftarrow \mathcal{H}_3(U \| S \| \textsc{trans} \| X^b \| Y^b \| \mathsf{MS}')$

and accept.

V_{U_i} →

If $V_{U_i} \ne \mathcal{H}_2(U \| S \| \textsc{trans} \| B^x \| B^y \| \mathsf{MS})$, reject.

Otherwise, $SK \leftarrow \mathcal{H}_3(U \| S \| \textsc{trans} \| B^x \| B^y \| \mathsf{MS})$

and accept.

Fig. 2 An extension of the VEAP protocol where $\textsc{trans} = A \| A^x \| X \| B \| Y \| \{C_j\}_{1 \le j \le n}$

Extension 2: New PAKE

- By stripping off anonymity

User U_i (pw_i)

$a \stackrel{R}{\leftarrow} \mathbb{Z}_p^\star$, $W_i \leftarrow \mathcal{G}(U_i, pw_i)$,

$A \equiv W_i \times g^a$

$\xrightarrow{U_i, A}$

Server S $((U_j, pw_j),\ 1 \leq j \leq n)$

$x \stackrel{R}{\leftarrow} \mathbb{Z}_p^\star$, $X \equiv g^x$

For $i = j$, $W_j \leftarrow \mathcal{G}(U_j, pw_j)$ and $K_j \equiv (W_j)^x$.

Compute A^x

$V_S \leftarrow \mathcal{H}_1(U_i \| S \| A \| A^x \| X \| W_j \| K_j)$

$\xleftarrow{S, X, A^x, V_S}$

$K_i \equiv A^x / X^a$,

If $V_S \neq \mathcal{H}_1(U_i \| S \| A \| A^x \| X \| W_i \| K_i)$, reject.

Otherwise, $V_{U_i} \leftarrow \mathcal{H}_2(U_i \| S \| A \| A^x \| X \| W_i \| K_i)$

$SK \leftarrow \mathcal{H}_3(U_i \| S \| A \| A^x \| X \| W_i \| K_i)$

and accept.

$\xrightarrow{V_{U_i}}$

If $V_{U_i} \neq \mathcal{H}_2(U_i \| S \| A \| A^x \| X \| W_j \| K_j)$, reject.

Otherwise, $SK \leftarrow \mathcal{H}_3(U_i \| S \| A \| A^x \| X \| W_j \| K_j)$

and accept.

Fig. 3 A new PAKE protocol from the VEAP protocol

Leakage-Resilient AKE

Previous AKE Protocols

- Security under the assumption
  - **Stored secrets are secure**
  - E.g., secret keys, private keys, verification data for passwords/biometrics
- What happens if stored secrets are leaked?

Leakage of Stored Secrets/Data

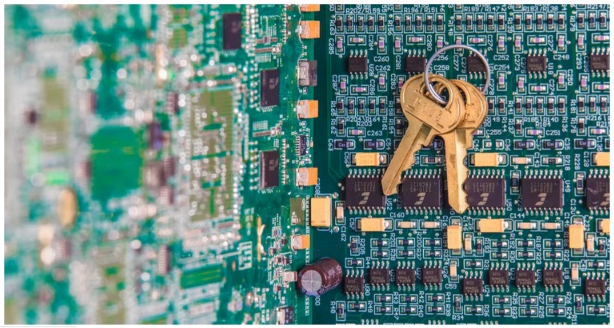
- Very common
  - No perfect TRM/TPM
  - Lost/stolen devices
  - Unauthorized access (hacking), virus
  - Server admin.'s misconduct, misconfiguration
  - …
- Practical threats in the real world
  - https://en.wikipedia.org/wiki/List_of_data_breaches
  - https://haveibeenpwned.com/
  - https://www.avast.com/hackcheck

Your Passwords?

Massive breach leaks 773 million email addresses, 21 million passwords

The best time to stop reusing old passwords was 10 years ago. The second best time is now.

Alfred Ng Jan. 17, 2019 8:40 a.m. PT

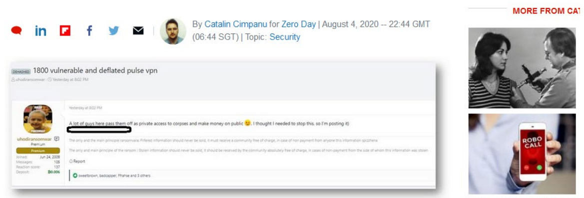


https://www.cnet.com/news/massive-breach-leaks-773-million-emails-21-million-passwords/

Hacker leaks passwords for 900+ enterprise VPN servers

EXCLUSIVE: The list has been shared on a Russian-speaking hacker forum frequented by multiple gangs.

By Catalin Cimpanu for Zero Day | August 4, 2020 -- 22:44 GMT (06:44 SGT) | Topic: Security

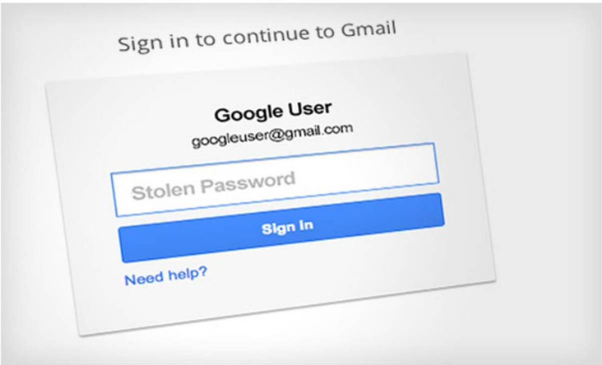


https://www.zdnet.com/article/hacker-leaks-passwords-for-900-enterprise-vpn-servers/

5 Million Google Passwords Leaked

Stolen Credentials Surface on Russian Cybercrime Forums

Mathew J. Schwartz (euroinfosec) • September 10, 2014



https://www.bankinfosecurity.com/5-million-google-passwords-leaked-a-7299

Hackers Dump 2.2M Gaming, Cryptocurrency Passwords Online

https://threatpost.com/hackers-dump-2-2m-gaming-cryptocurrency-passwords-online/150451/

https://www.cpomagazine.com/cyber-security/another-instagram-password-leak-third-party-follower-bot-exposes-plaintext-credentials-of-thousands-of-accounts/

15 Billion Credentials Currently Up for Grabs on Hacker Forums

https://threatpost.com/15-billion-credentials-currently-up-for-grabs-on-hacker-forums/157247/

AIST

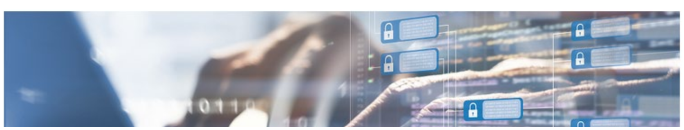
Your Passwords!

- How many passwords do you remember?
  - If a user registers the same (or similar) password to different servers, …
  - Password list attacks (credential stuffing)

Recent Trends in Password List Attacks and Countermeasures

by Yoshitaka Nakahara Cloud Security

2step verification, bad bot, Bot detection, BotGuard, brute force attacks, CDN, Cloud Security, dictionary attacks, password list attacks, web security, zero-day



https://www.cdnetworks.com/cloud-security-blog/recent-trends-in-password-list-attacks-and-countermeasures/

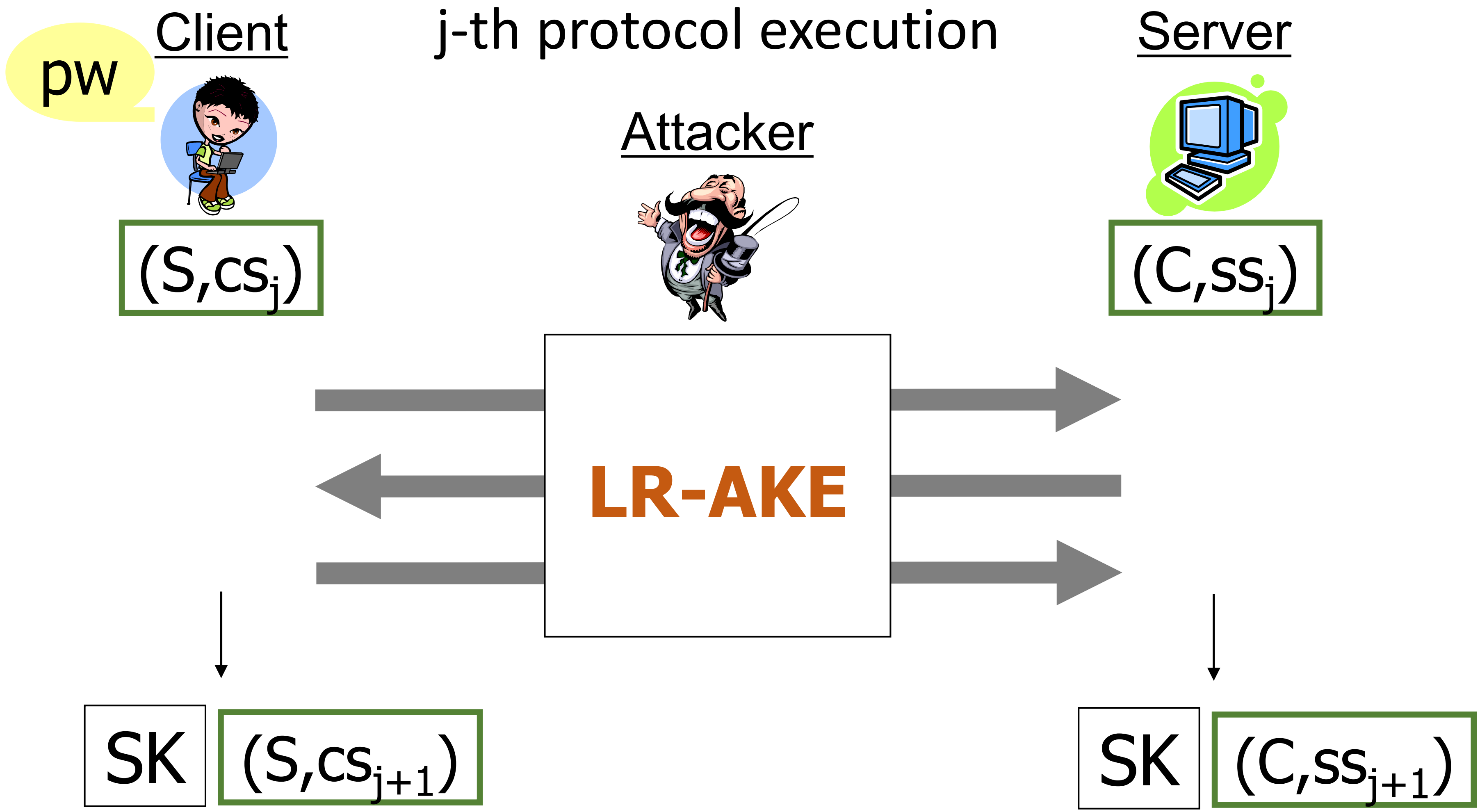
  - LastPass, 1Password and other password managers can be hacked: What to do now (March 25, 2020) https://www.tomsguide.com/news/password-manager-hacks

Leakage-Resilient AKE (LR-AKE)

- LR-AKE
  - New concept of AKE
  - **A maximum level of security**
    - Against active attacks as well as leakage of stored secrets
  - DL-based [**S**KI03, **S**KI05], RSA-based [**S**KI07]

[**S**KI03] **S. H. Shin**, K. Kobara, and H. Imai, "Leakage-Resilient Authenticated Key Establishment Protocols," ASIACRYPT 2003
[**S**KI05] **S. H. Shin**, K. Kobara, and H. Imai, "A Simple Leakage-Resilient Authenticated Key Establishment Protocol, Its Extensions, and Applications," IEICE Transactions, 2005
[**S**KI07] **S. H. Shin**, K. Kobara, and H. Imai, "An Efficient and Leakage-Resilient RSA-Based Authenticated Key Exchange Protocol with Tight Security Reduction," IEICE Transactions, 2007

Concept of LR-AKE



RSA-Based LR-AKE [SKI07]

j-th protocol execution

Client

pw

$(S, RSAPK, cs_j)$

Server

$(C, RSASK, ss_j)$

Client → Server: $E_{RSAPK}(z) \cdot H(pw + cs_j)$

Server → Client: $H1(z)$

Client → Server: $H2(z)$

Client: $SK = H3(z)$

Server: $SK = H3(z)$

Client: $(S, RSAPK, cs_{j+1} = cs_j + H4(z))$

Server: $(C, RSASK, ss_{j+1} = ss_j + H4(z))$

Comparison

AKE Protocols	Eaves dropping	Parallel on-line attacks	Leakage from client	Leakage from server	Leakage from both with different time-slots	Phishing attacks	No. of PW
CHAP etc.	NO	NO	OK	NO	NO	OK	Multiple
PAKE	OK	NO	OK	NO	NO	OK	Multiple
PKI (server PK auth. + PW)	OK	NO	OK	NO	NO	NO	Multiple
PKI (server PK auth. + PW + token)	OK	OK	OK	NO	NO	NO	Multiple
PKI (mutual PK auth.)	OK	OK	NO	OK	NO	NO	Only one
LR-AKE	OK	OK	OK	OK	OK	OK	Only one

AIST

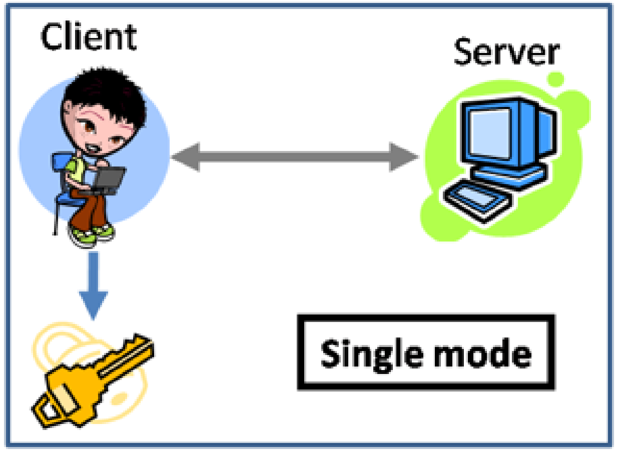
Other Advantages

- Another layer of security
  - (Serial) **online dictionary attacks are not possible**
  - **Automatic revocation** of leaked secrets
- High efficiency
  - Especially, **client side** [**S**KI07]
- **'Strong' forward secrecy**
- **No management** of PK certificates

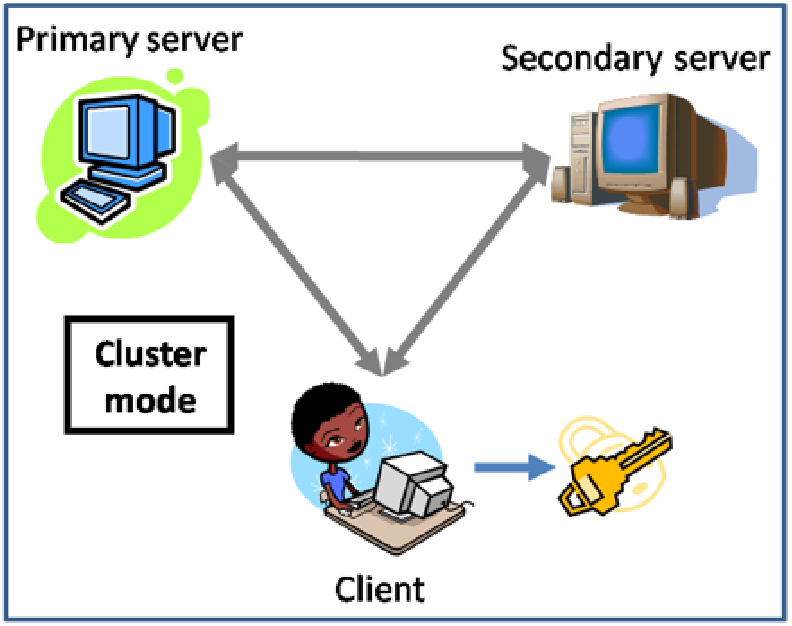
AIST

Extension to Data Security

- Online data key recovery
  - Strengthened by LR-AKE
- Single mode



- Cluster mode [I**S**K09]



[I**S**K09] H. Imai, **S. H. Shin**, and K. Kobara, “New Security Layer for OverLay Networks (Invited Paper),” Journal of Communications and Networks, 2009

Applications

- Any authentication or data storage service
  - Login to remote server/intranet/hotspot, …
  - SSH, VPN, authentication for thin client, …
  - Webmail, online shopping, Internet banking, …
  - Identity management, SSO (on client side), …
  - Credential-retrieval systems, …
  - NAS, cloud storage system, …
  - Online distributed storage system, …

ISO/IEC 11770-4:2017/AMD 2 [ISO/IEC11770-4Amd2]

- Leakage-Resilient Key Agreement Mechanism
  - LKAM1 [**S**KI08b]
  - LKAM2 [**S**KI10b]

[ISO/IEC11770-4Amd2] ISO/IEC 11770-4:2017/AMD 2, “Information technology – Security techniques – Key management – Part 4: Mechanisms based on weak secrets – Amendment 2: Leakage-resilient password-authenticated key agreement with additional stored secrets,” 2021
[**S**KI08b] **S. H. Shin**, K. Kobara, and H. Imai, “A Secure Authenticated Key Exchange Protocol for Credential Services,” IEICE Transactions, 2008
[**S**KI10b] **S. H. Shin**, K. Kobara, and H. Imai, “An RSA-Based Leakage-Resilient Authenticated Key Exchange Protocol Secure against Replacement Attacks, and Its Extensions,” IEICE Transactions, 2010

Hybrid AKE

Motivation

- Identity-based PAKE (called, iPAKE) [CCH+15]
  - Using the Boneh-Franklin IBE [BF01, BF03]
- Its generic construction [CCH+15]
  - Using an identity-based KEM/DEM scheme [Boy08]
  - **Standardized in ISO/IEC 11770-4/AMD 1**
    - Named as 'Unbalanced Key Agreement Mechanism with Password and Identity-based Encryption (UKAM-PiE)'

[CCH+15] K. Y. Choi et al., "Constructing Efficient PAKE Protocols from Identity-Based KEM/DEM," WISA 2015

Our Contributions [**S**22]

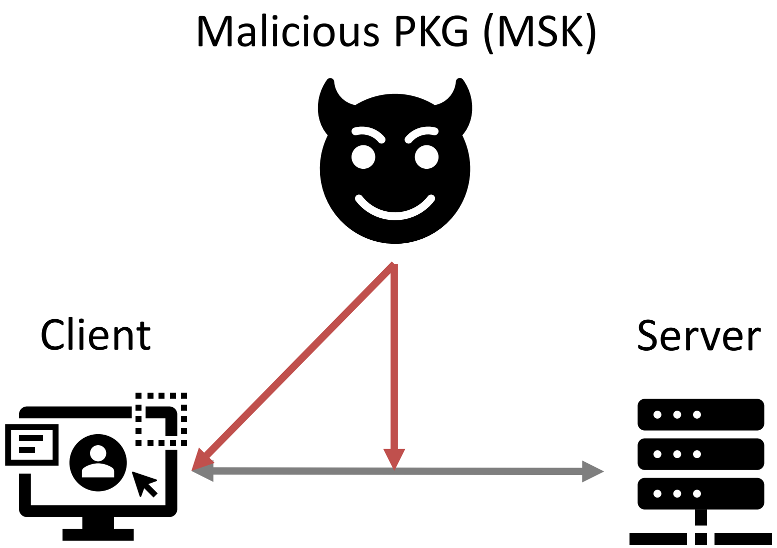
- **Security analysis** of iPAKE and UKAM-PiE
  - Insecure against passive/active attacks by a malicious PKG (Private Key Generator)
    - C.f., “Mechanisms to prevent access to keys by third parties,” Annex D of ISO/IEC 18033-5
    - Key escrow problem in IBE, HIBE (Hierarchical IBE), …
  - Can find out all clients’ passwords by just eavesdropping
  - Can share a session key with any client by impersonating the server

- Propose a strengthened PAKE (for short, **SPAIBE**) protocol with IBE
  - Preventing such malicious PKG’s attacks
  - Formally prove the security of SPAIBE in the RO model
  - Compare with relevant protocols

[**S**22] **S. H. Shin**, “A Strengthened PAKE Protocol with Identity-Based Encryption,” IEICE Transactions on Information and Systems, November 2022

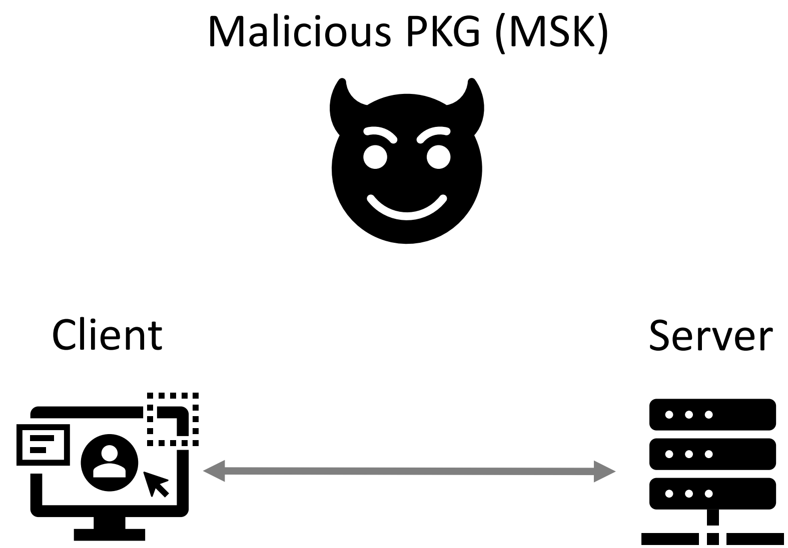
Security against Malicious PKG (Compromise of Master Secret Key)

- UKAM-PiE



  - Offline dictionary attacks
  - Server impersonation attacks

- **SPAIBE**



  - **Offline dictionary attacks and server impersonation attacks are not possible**

SPAIBE

Public parameters (pp): $\mathbb{G}_1, \mathbb{G}_2, e, q, g, h, \underbrace{g^z}_{\mathsf{mpk}}, G, H, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3$

Client $\mathsf{C}\ (pw)$

Server $\mathsf{S}\ \left(d_{\mathsf{S}}, \left(\mathsf{C}, h^{-\mathsf{H}_1(pw)}\right)\right)$

Key Establishment

Client:

$x \stackrel{\$}{\leftarrow} \mathbb{Z}_q^\star,\ X \equiv g^x$

$W \equiv X \cdot h^{\mathsf{H}_1(pw)}$

$r \stackrel{\$}{\leftarrow} \mathbb{Z}_q^\star,\ g_{\mathsf{S}} = e(G(\mathsf{S}), g^z)$

$U_1 \equiv g^r,\ U_2 = W \oplus H(g_{\mathsf{S}}^r)$

Double-masking

$\mathsf{Encrypt}(pp_{\mathsf{IBE}}, \mathsf{S}, W)$ of BF-IBE

Client → Server: C, U_1, U_2

Server:

$y \stackrel{\$}{\leftarrow} \mathbb{Z}_q^\star,\ Y \equiv g^y$

$\mathsf{Decrypt}(pp_{\mathsf{IBE}}, (U_1, U_2), d_{\mathsf{S}})$ of BF-IBE

$\delta = e(d_{\mathsf{S}}, U_1)$

$W = U_2 \oplus H(\delta)$

$X' \equiv W \cdot h^{-\mathsf{H}_1(pw)},\ K' \equiv (X')^y$

$sid = \mathsf{C}||\mathsf{S}||U_1||U_2||Y$

$V_{\mathsf{S}} = \mathsf{H}_2(sid||X'||K')$

$SK_{\mathsf{S}} = \mathsf{H}_3(sid||X'||K')$

Server → Client: $\mathsf{S}, Y, V_{\mathsf{S}}$

Server authenticator

Client:

$sid = \mathsf{C}||\mathsf{S}||U_1||U_2||Y$

$K \equiv Y^x$

If $V_{\mathsf{S}} \neq \mathsf{H}_2(sid||X||K)$, abort.

Otherwise, $SK_{\mathsf{C}} = \mathsf{H}_3(sid||X||K)$.

Security of SPAIBE

- Security proof in the RO model

Theorem 1: Let P be the SPAIBE protocol of Fig. 1 where passwords are chosen from a dictionary of size N. For any adversary $\mathcal{A}$ within a polynomial time t, with less than q_{se} active interactions with the parties (Send-queries), q_{ex} passive eavesdroppings (Execute-queries) and asking q_{H} hash queries to any H_j, $\mathsf{Adv}_P^{\mathsf{ake}}(\mathcal{A}) \leq \varepsilon$, with ε upper-bounded by

$$\frac{6q_{\mathsf{se}}}{N} + 6q_{\mathsf{H}}^2 \times \mathsf{Succ}_{\mathbb{G}_1}^{\mathsf{cdh}}(t_1 + 3\tau_e) + \frac{3\,(q_{\mathsf{ex}} + q_{\mathsf{se}})^2}{q} + \frac{2q_{\mathsf{se}}}{2^k} + 4nq_{\mathsf{se}} \times \mathsf{Adv}_{IBE}^{\mathsf{ind\text{-}id\text{-}cpa}}(\mathcal{B})\,, \qquad (2)$$

Comparison

- Almost same efficiency as UKAM-PiE

Table 1 Comparison of PAKE protocols using the BF-IBE scheme [15], [18]

Protocols	Computation costs		Communication costs	# of passes	Security against a malicious PKG
	Client C	Server S			
PAKE-CS [17]	$1\text{Pairing} + 5\text{Exp}_{\mathbb{G}_1} + 1\text{Exp}_{\mathbb{G}_2}$	$1\text{Pairing} + 4\text{Exp}_{\mathbb{G}_1}$	$\|\|C\|\| + \|\|S\|\| + 4\|\|\mathbb{G}_1\|\| + \|\|H\|\|$	2	No
iPAKE [2]	$1\text{Pairing} + 2\text{Exp}_{\mathbb{G}_1} + 1\text{Exp}_{\mathbb{G}_2}$	$1\text{Pairing} + 2\text{Exp}_{\mathbb{G}_1}$	$\|\|C\|\| + \|\|S\|\| + 2\|\|\mathbb{G}_1\|\| + \|\|H\|\|$	2	No
UKAM-PiE [21]	$1\text{Pairing} + 3\text{Exp}_{\mathbb{G}_1} + 1\text{Exp}_{\mathbb{G}_2}$	$1\text{Pairing} + 2\text{Exp}_{\mathbb{G}_1}$	$\|\|C\|\| + \|\|S\|\| + 2\|\|\mathbb{G}_1\|\| + \|\|H\|\|$	2	No
SPAIBE (Sect. 5)	$1\text{Pairing} + 3.17\text{Exp}_{\mathbb{G}_1} + 1\text{Exp}_{\mathbb{G}_2}$	$1\text{Pairing} + 2\text{Exp}_{\mathbb{G}_1}$	$\|\|C\|\| + \|\|S\|\| + 2\|\|\mathbb{G}_1\|\| + 2\|\|H\|\|$	2	Yes

ISO/IEC JTC 1/SC 27/WG 2 Meeting

- Redmond, Washington, USA
- 18th – 21st April, 2023

- Japan National Body’s contribution
  - N 3184, “A Proposal to Include SPAIBE to ISO/IEC 11770-4”
- Agreed to initiate a PWI on Inclusion of SPAIBE in ISO/IEC 11770-4
  - Editor: **S. H. Shin**, Co-editor: K. Kobara

Applications

Applications of AKE

- Authentication service
- Wireless security
- Cryptocurrency
  - Coincheck hack (2018-01)
- Cyber-physical security
- SNS
  - Signal, LINE
- …

Thank you for your attention!!

SeongHan Shin

CPSEC, AIST

seonghan.shin@aist.go.jp