Public-Key Encryption Indistinguishable Under Plaintext-Checkable Attacks

Michel Abdalla, *Fabrice Benhamouda*, and David Pointcheval

École Normale Supérieure, CNRS, INRIA, PSL, Paris, France

PKC 2015 — Maryland, USA
Tuesday, March 31

Motivation: Encryption Schemes under Plain DDH

Cyclic group $\mathbb{G}$ order p. Message $M \in \mathbb{G}$

	ElGamal
public key pk	$g,\ h$ $\in \mathbb{G}^2$
ciphertext c	$g^r,\ h^r \cdot M$ $\in \mathbb{G}^2$
security	IND-CPA ind. under chosen-plaintext attacks

Motivation: Encryption Schemes under Plain DDH

Cyclic group $\mathbb{G}$ order p. Message $M \in \mathbb{G}$

ElGamal

public key pk: $g, h \in \mathbb{G}^2$

ciphertext c: $g^r, h^r \cdot M \in \mathbb{G}^2$

security: IND-CPA

ind. under chosen-plaintext attacks

Motivation: Encryption Schemes under Plain DDH

Cyclic group $\mathbb{G}$ order p. Message $M \in \mathbb{G}$

	ElGamal	**Cramer-Shoup**
public key pk	$g,\ h$ $\in \mathbb{G}^2$	$g_1,\ g_2,\ h,\ c,\ d$ $\in \mathbb{G}^5$
ciphertext c	$g^r,\ h^r \cdot M$ $\in \mathbb{G}^2$	${g_1}^r,\ {g_2}^r,\ h^r \cdot M,\ (cd^{\xi})^r$ $\in \mathbb{G}^4$ $(\xi = H({g_1}^r, {g_2}^r, h^r \cdot M))$
security	IND-CPA ind. under chosen-plaintext attacks	IND-CCA ind. under chosen-ciphertext attacks

Motivation: Encryption Schemes under Plain DDH

Cyclic group $\mathbb{G}$ order p. Message $M \in \mathbb{G}$

	ElGamal		**Cramer-Shoup**
public key pk	$g,\ h$ $\in \mathbb{G}^2$		$g_1,\ g_2,\ h,\ c,\ d$ $\in \mathbb{G}^5$
ciphertext c	$g^r,\ h^r \cdot M$ $\in \mathbb{G}^2$	?	${g_1}^r,\ {g_2}^r,\ h^r \cdot M,\ (cd^\xi)^r$ $\in \mathbb{G}^4$ $(\xi = H({g_1}^r, {g_2}^r, h^r \cdot M))$
security	IND-CPA ind. under chosen-plaintext attacks		IND-CCA ind. under chosen-ciphertext attacks

Motivation: Encryption Schemes under Plain DDH

Cyclic group $\mathbb{G}$ order p. Message $M \in \mathbb{G}$

	ElGamal	**Short Cramer-Shoup**	**Cramer-Shoup**
public key pk	$g,\ h$ $\in \mathbb{G}^2$	$g,\ h,\ c,\ d$ $\in \mathbb{G}^4$	$g_1,\ g_2,\ h,\ c,\ d$ $\in \mathbb{G}^5$
ciphertext c	$g^r,\ h^r \cdot M$ $\in \mathbb{G}^2$	$g^r,\ h^r \cdot M,\ (cd^\xi)^r$ $\in \mathbb{G}^3$ $(\xi = H(g^r, h^r \cdot M))$	${g_1}^r,\ {g_2}^r,\ h^r \cdot M,\ (cd^\xi)^r$ $\in \mathbb{G}^4$ $(\xi = H({g_1}^r, {g_2}^r, h^r \cdot M))$
security	IND-CPA	IND-PCA	IND-CCA
	ind. under chosen-plaintext attacks	ind. under plaintext-checkable [OP01] attacks	ind. under chosen-ciphertext attacks

Table of Contents

1. IND-PCA Security Notion
   - Definitions of IND-CPA, IND-CCA, and IND-PCA
   - Relations between Security Notions
   - Applications
2. Short Cramer-Shoup
   - Scheme
   - Security Proof
3. Application to PAKE
   - Definition of PAKE
   - Constructions

Encryption Scheme

$(pk, sk) \xleftarrow{\$} \mathsf{KG}(1^{\mathfrak{K}})$ generates a key pair (pk, sk)

$c \xleftarrow{\$} \mathsf{Enc}(pk, M)$ encrypts the plaintext M

$M \leftarrow \mathsf{Dec}(sk, c)$ decrypts the ciphertext c

Encryption Scheme

$(pk, sk) \xleftarrow{\$} \mathsf{KG}(1^{\mathfrak{K}})$ generates a key pair (pk, sk)

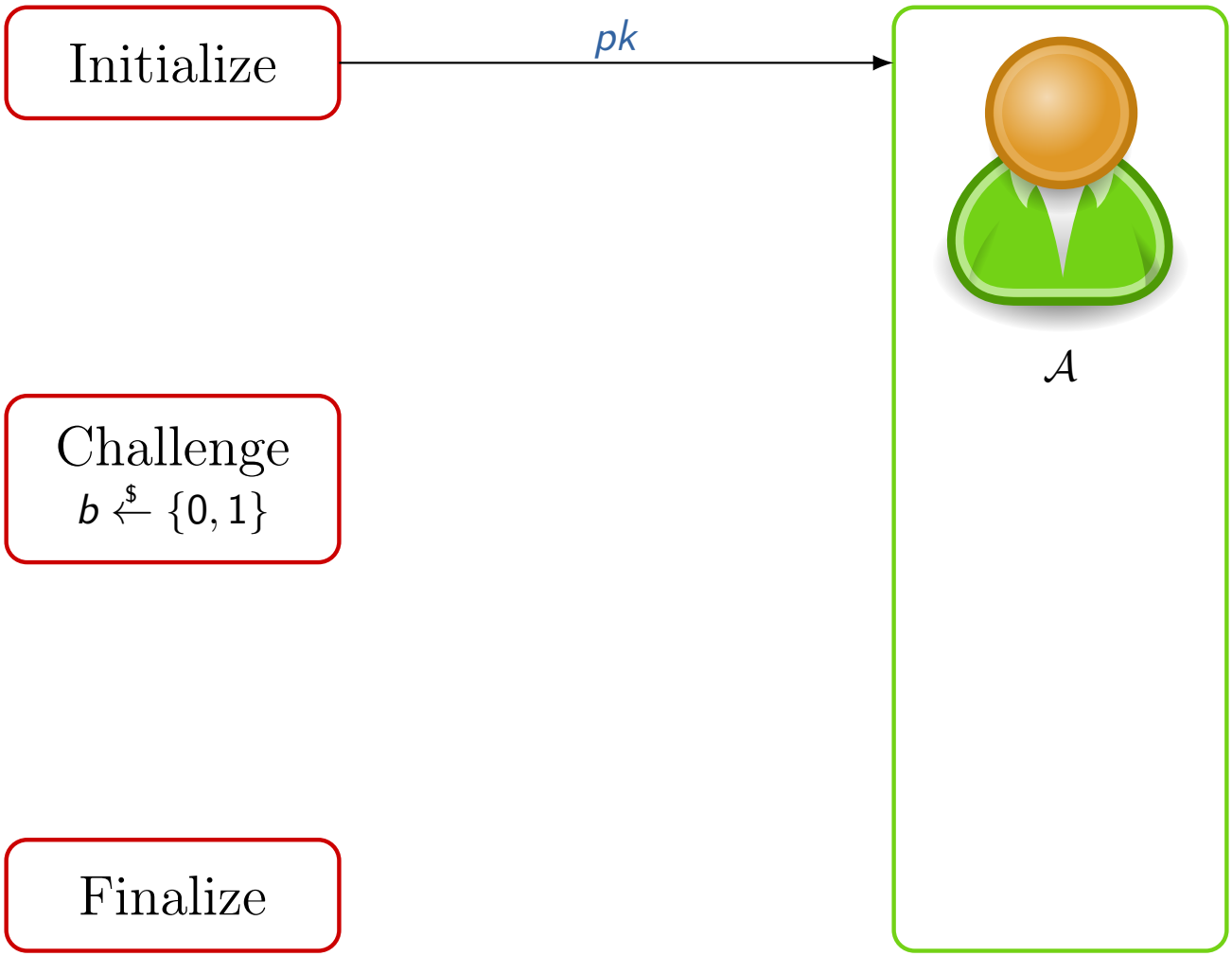
$c \xleftarrow{\$} \mathsf{Enc}(pk, M)$ encrypts the plaintext M

$M \leftarrow \mathsf{Dec}(sk, c)$ decrypts the ciphertext c

Correctness: if $(pk, sk) \xleftarrow{\$} \mathsf{KG}(1^{\mathfrak{K}})$,

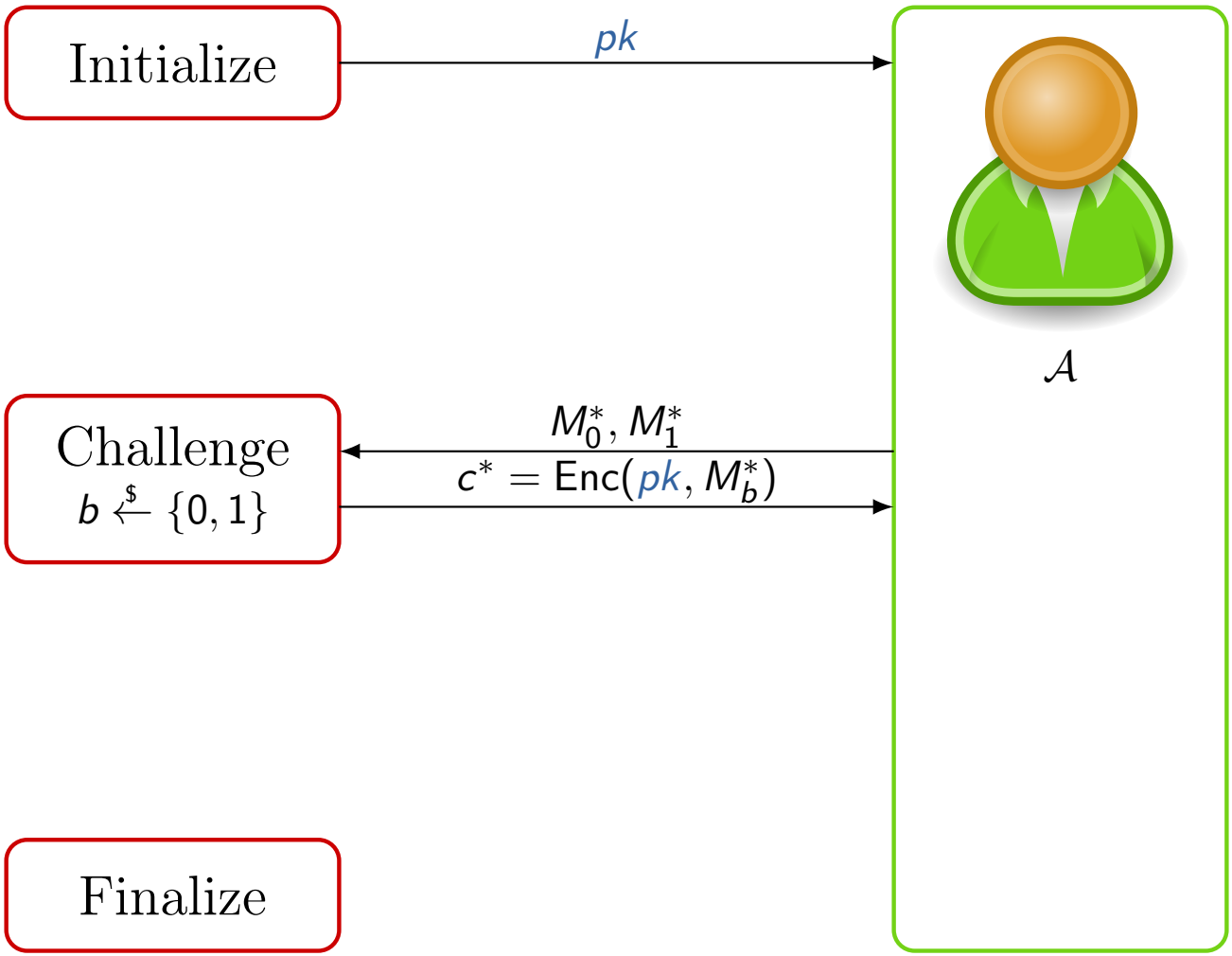
$$\mathsf{Dec}(sk, \mathsf{Enc}(pk, M)) = M.$$

IND-**CPA** Security Notion



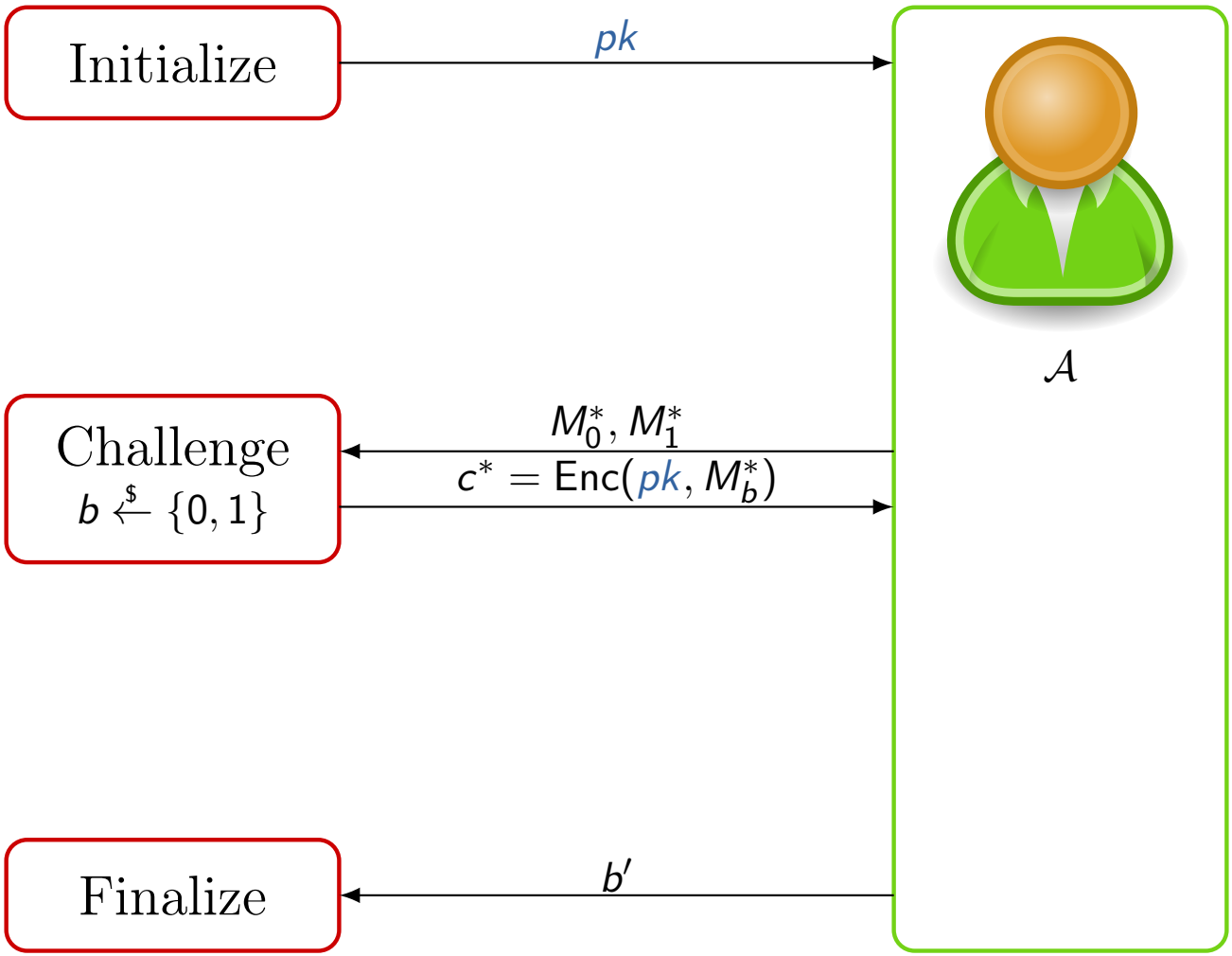
Advantage: $2\Pr[b = b'] - 1$.

IND-**CPA** Security Notion



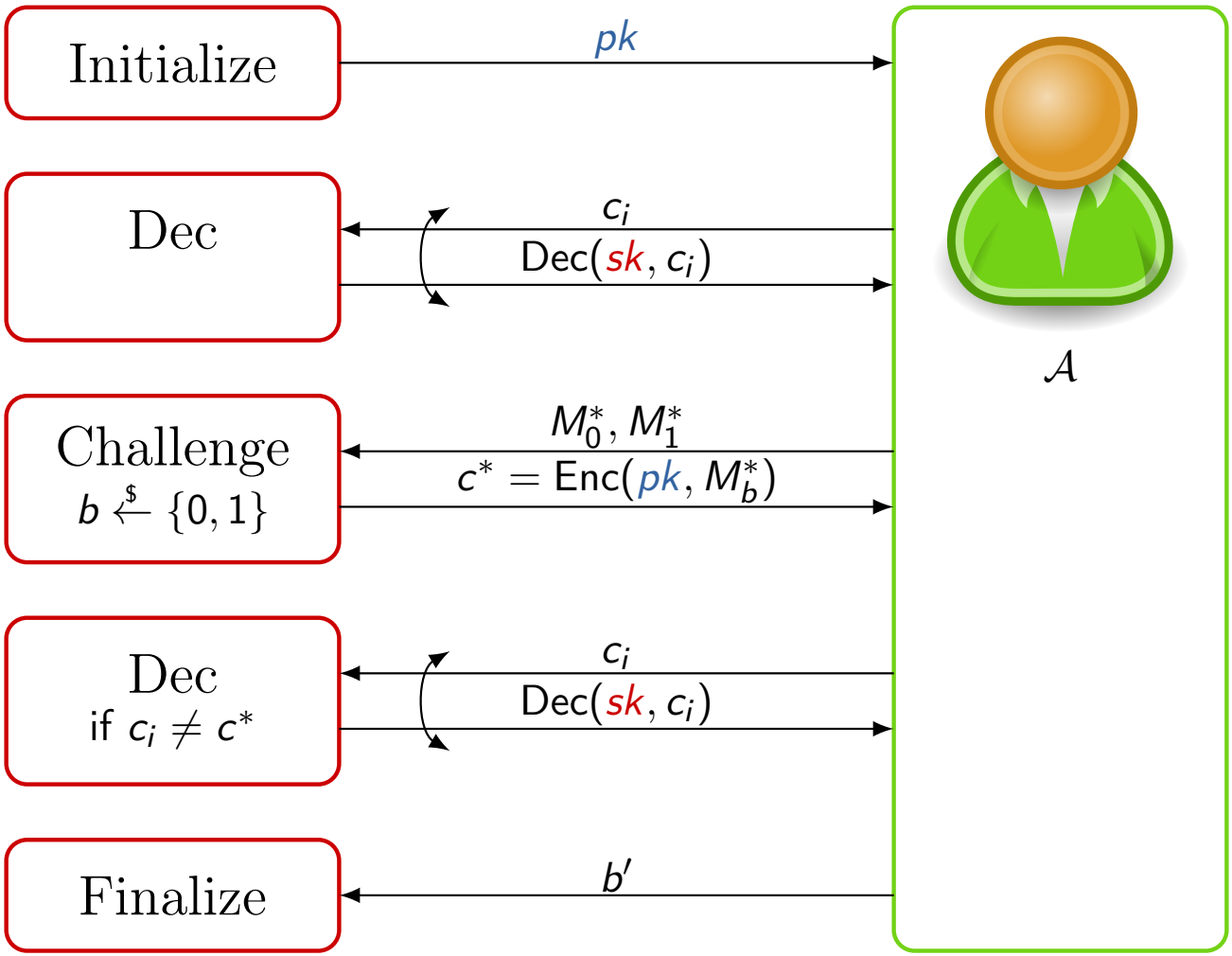
Advantage: $2\Pr[b = b'] - 1$.

IND-**CPA** Security Notion



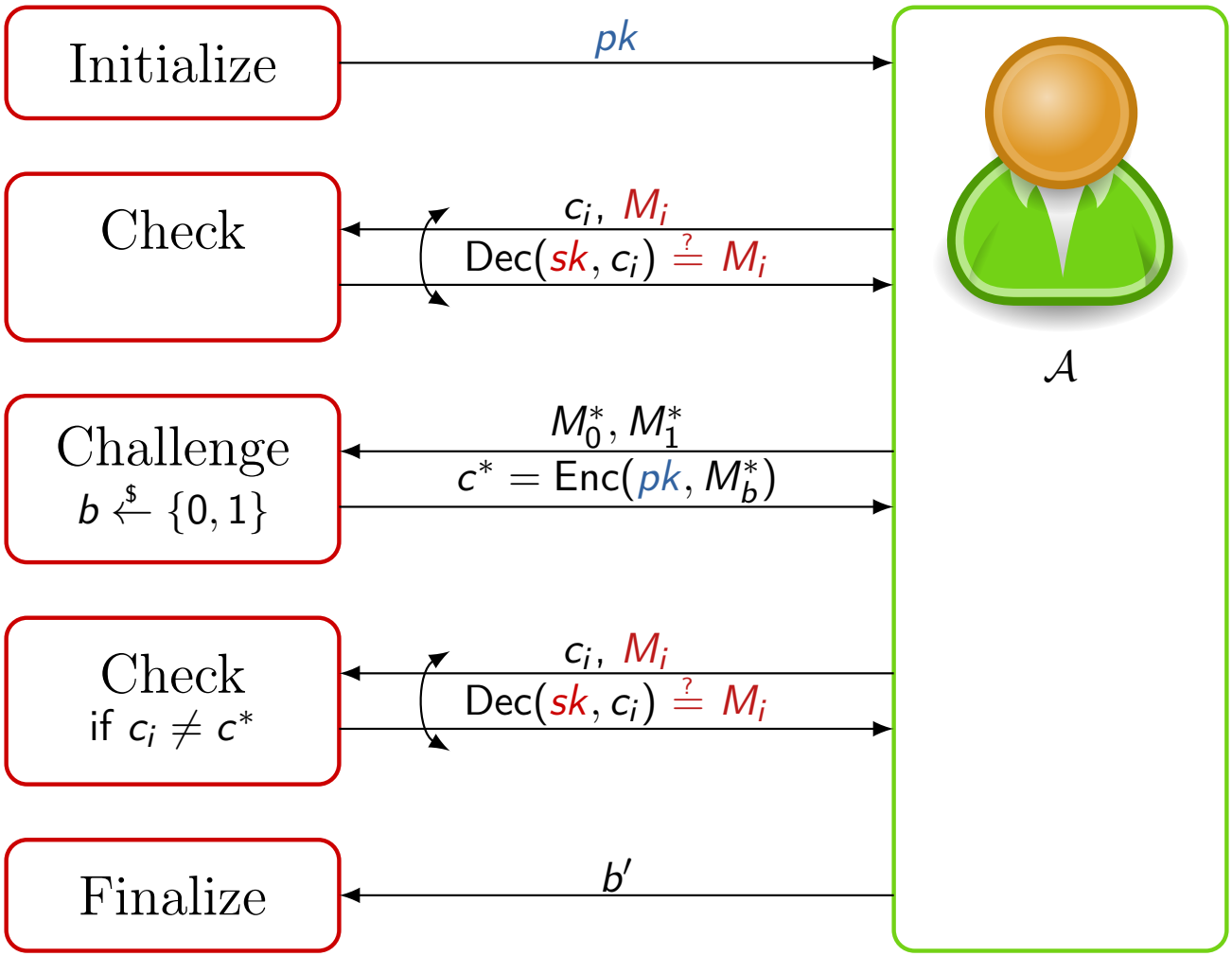
Advantage: $2\Pr[b = b'] - 1$.

IND-**CCA** Security Notion



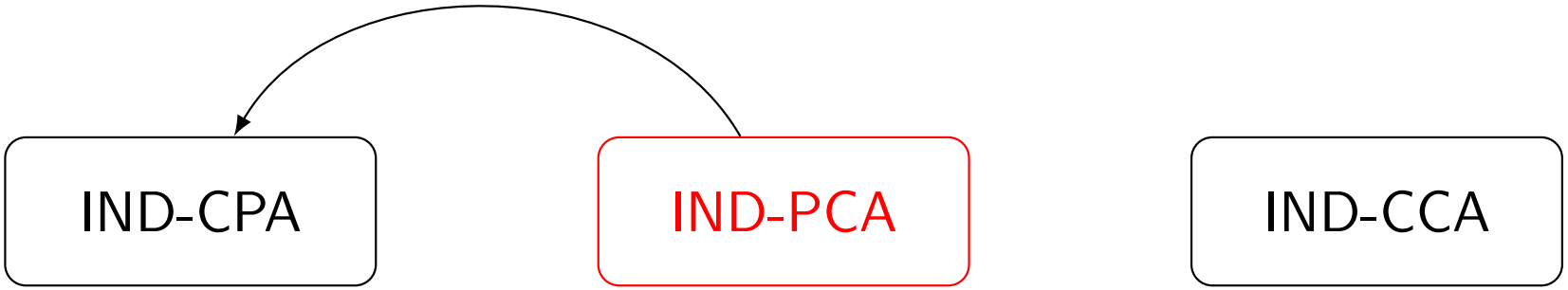
Advantage: $2\Pr[b = b'] - 1$.

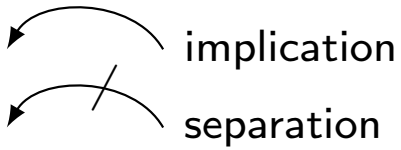
IND-**PCA** Security Notion



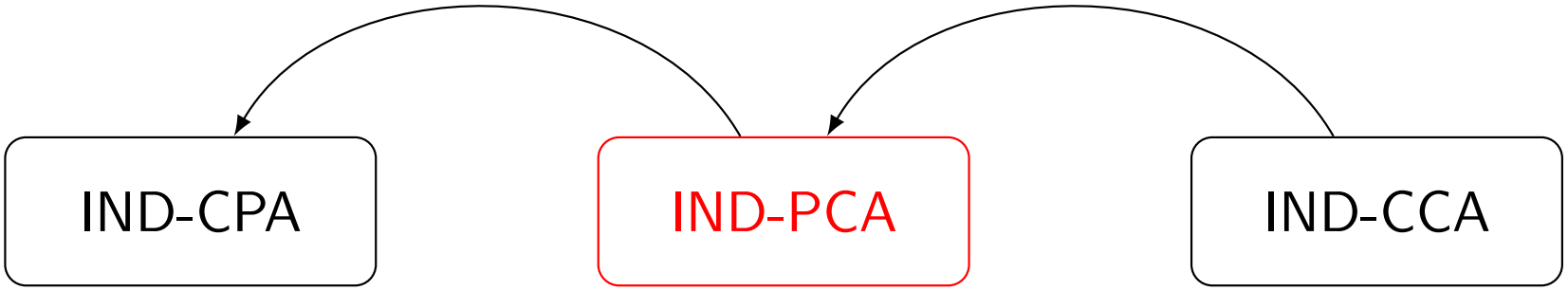
Advantage: $2\Pr[b = b'] - 1$.

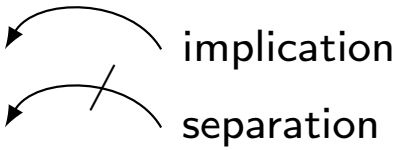
Relations between Security Notions



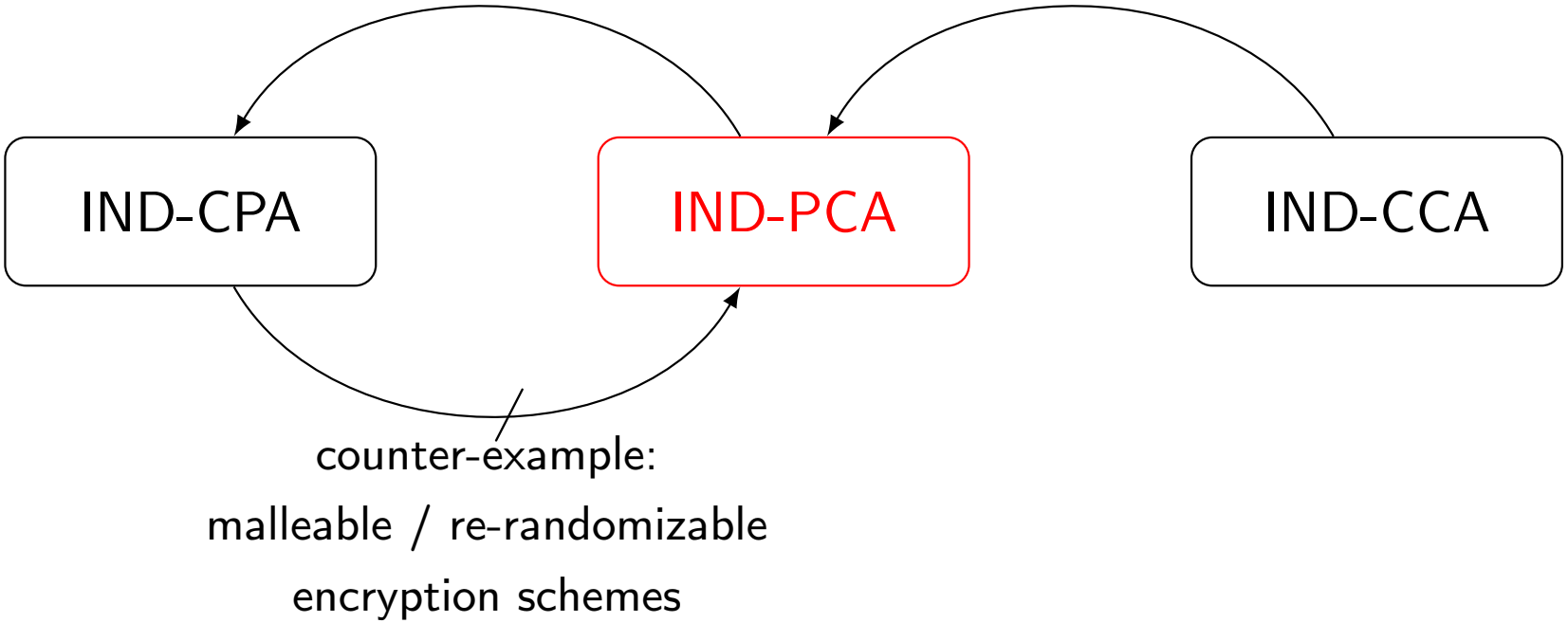


Relations between Security Notions

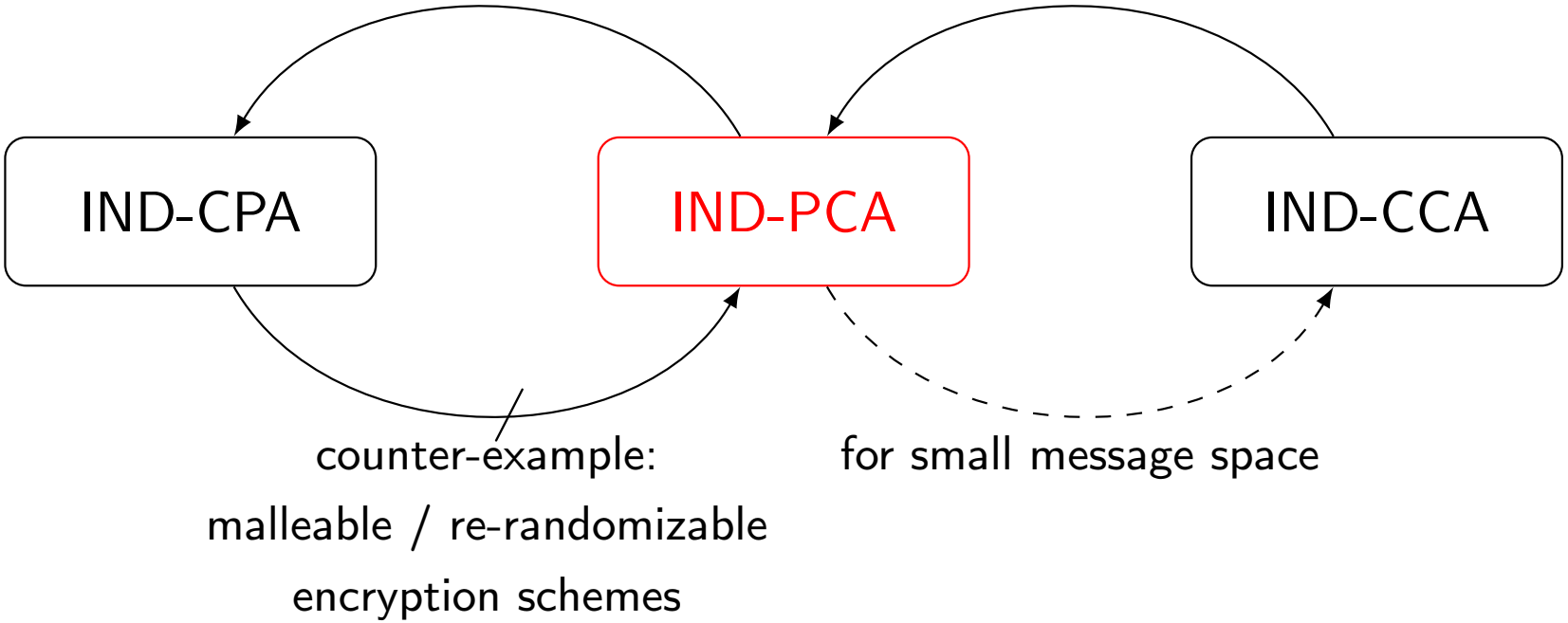




Relations between Security Notions



Relations between Security Notions



Applications of IND-PCA Schemes

- IND-CCA encryption with small message space
  - encryption of small passwords (e.g., PIN)
- IND-CCA encryption of bits
  - OT protocols based on hash proof systems [BBC+13]
  - bit-by-bit encryption of scalars
    e.g., Groth-Sahai proofs [GS08], blind signatures [BPV12], ...
- Direct use in PAKE schemes

Short Cramer-Shoup Encryption Scheme

- $\mathbb{G}$ cyclic group of order p, generator g;
- H: collision-resistant hash function;
- Key generation:

$$sk = (s,\ a,\ b,\ a',\ b') \xleftarrow{\$} \mathbb{Z}_p^5$$

$$pk = \left(g,\ h = g^s,\ c = g^a h^b,\ d = g^{a'} h^{b'}\right) \in \mathbb{G}^4$$

- Encryption of M: $r \xleftarrow{\$} \mathbb{Z}_p$

$$c \leftarrow \left(u = g^r,\ e = h^r \cdot M,\ v = \left(cd^{\xi}\right)^r\right) \in \mathbb{G}^3$$

with $\xi = H(u, e)$.

- Decryption of $c = (u, e, v)$:

$$M \leftarrow e/u^s \quad \text{and abort if } v \neq u^{a+\xi a'} \cdot (e/M)^{b+\xi b'}$$

Short Cramer-Shoup Encryption Scheme

- $\mathbb{G}$ cyclic group of order p, generator g;
- H: collision-resistant hash function;
- Key generation:

$$sk = (s,\ a,\ b,\ a',\ b') \xleftarrow{\$} \mathbb{Z}_p^5$$

$$pk = \left(g,\ h = g^s,\ c = g^a h^b,\ d = g^{a'} h^{b'}\right) \in \mathbb{G}^4$$

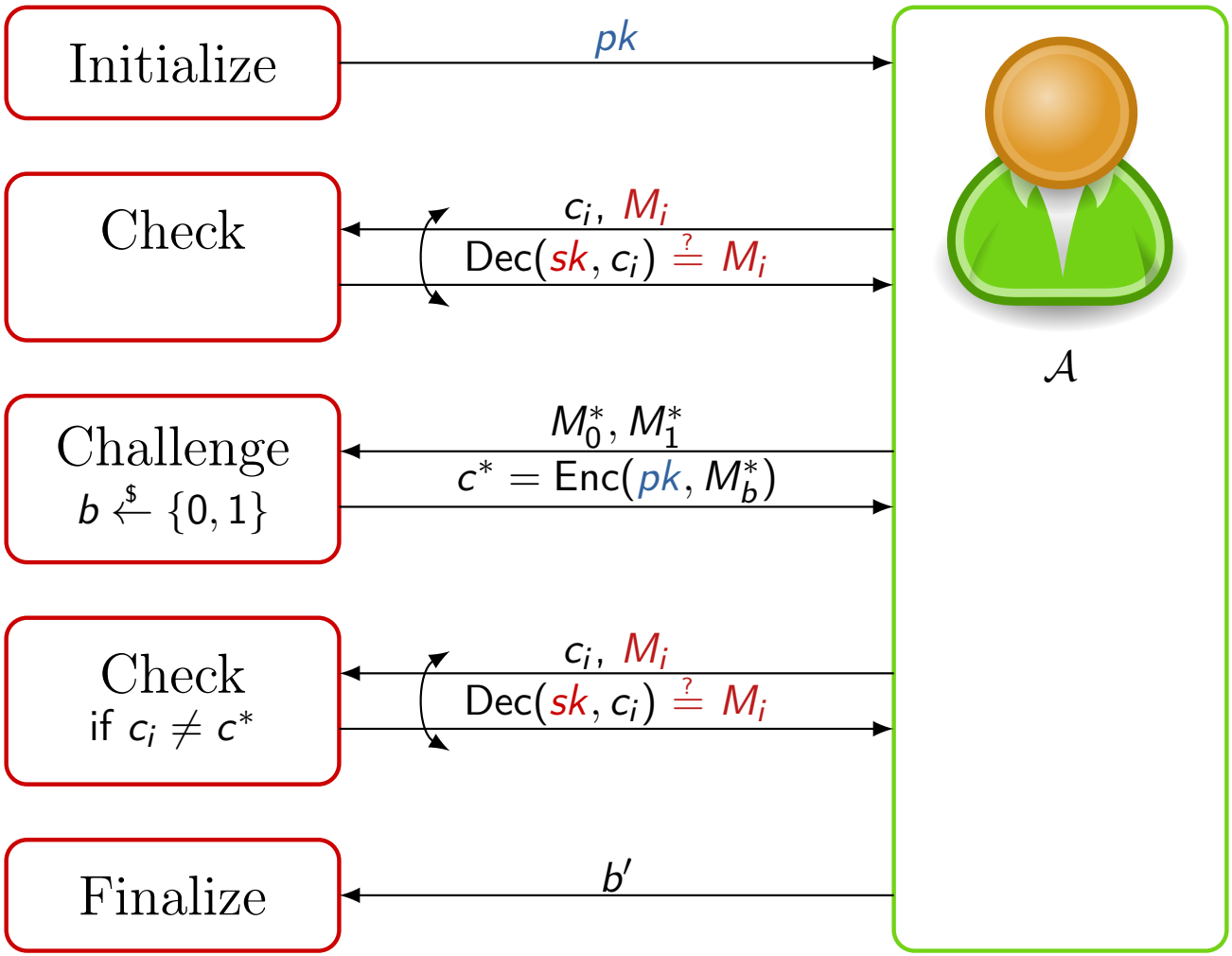
- Encryption of M: $r \xleftarrow{\$} \mathbb{Z}_p$

$$c \leftarrow \left(\underbrace{u = g^r,\ e = h^r \cdot M}_{\text{ElGamal}},\ \underbrace{v = (cd^\xi)^r}_{\text{Proof}}\right) \in \mathbb{G}^3$$

  with $\xi = H(u, e)$.
- Decryption of $c = (u, e, v)$:

$$M \leftarrow e/u^s \quad \text{and abort if } v \neq u^{a+\xi a'} \cdot (e/M)^{b+\xi b'}$$

IND-**PCA** Security Notion



Advantage: $2\Pr[b = b'] - 1$.

Security Proof

Check $c_i = (u_i, e_i, v_i)$ is an encryption of M_i:

$$M_i \stackrel{?}{=} e_i / u_i^s \quad (1) \qquad v_i \stackrel{?}{=} u_i^{a+\xi_i a'} \cdot (e_i / M_i)^{b+\xi_i b'} \quad (2)$$

Challenge:

$$c^* = (u^*, e^*, v^*) = \left(g^{r^*},\ h^{r^*} \cdot M_b^*,\ (cd^{\xi^*})^{r^*} \right) \quad \text{with } \xi^* = H(u^*, e^*).$$

Security Proof

Check $c_i = (u_i, e_i, v_i)$ is an encryption of M_i:

$$M_i \stackrel{?}{=} e_i / u_i^s \quad (1) \qquad v_i \stackrel{?}{=} u_i^{a+\xi_i a'} \cdot (e_i/M_i)^{b+\xi_i b'} \quad (2)$$

Challenge:

$$c^* = (u^*, e^*, v^*) = \left(g^{r^*},\ h^{r^*} \cdot M_b^*,\ \left(cd^{\xi^*}\right)^{r^*}\right) \quad \text{with } \xi^* = H(u^*, e^*).$$

v: 2-universal hash proof [CS02]:

correctness if $u = g^r$ and $e = h^r \cdot M$:

$$(v =)\ \left(cd^{\xi}\right)^r = u^{a+\xi_i a'} \cdot (e/M)^{b+\xi b'}$$

2-universality for any u_i, e_i, if $M_i \neq e_i/u_i^s$:

$$u_i^{a+\xi_i a'} \cdot (e_i/M_i)^{b+\xi_i b'} \quad \approx \quad \$$$

even seeing $u^{*a+\xi^* a'} \cdot (e^*/M_b^*)^{b+\xi^* b'}$, for one (u^*, e^*).

Security Proof

Check $c_i = (u_i, e_i, v_i)$ is an encryption of M_i:

$$M_i \stackrel{?}{=} e_i / u_i^s \quad (1) \qquad v_i \stackrel{?}{=} u_i^{a+\xi_i a'} \cdot (e_i / M_i)^{b+\xi_i b'} \quad (2)$$

Challenge:

$$c^* = (u^*, e^*, v^*) = \left(g^{r^*},\ h^{r^*} \cdot M_b^*,\ (cd^{\xi^*})^{r^*} \right) \quad \text{with } \xi^* = H(u^*, e^*).$$

c^*			Check	
u^*	e^*	v^*	(1)	(2)
g^{r^*}	$h^{r^*} \cdot M_b^*$	$(cd^{\xi^*})^{r^*}$	✓	✓

Security Proof

Check $c_i = (u_i, e_i, v_i)$ is an encryption of M_i:

$$M_i \stackrel{?}{=} e_i / u_i^s \quad (1) \qquad v_i \stackrel{?}{=} u_i^{a+\xi_i a'} \cdot (e_i / M_i)^{b+\xi_i b'} \quad (2)$$

Challenge:

$$c^* = (u^*, e^*, v^*) = \left(g^{r^*},\ h^{r^*} \cdot M_b^*,\ \left(c d^{\xi^*}\right)^{r^*} \right) \quad \text{with } \xi^* = H(u^*, e^*).$$

c^*			Check	
u^*	e^*	v^*	(1)	(2)
g^{r^*}	$h^{r^*} \cdot M_b^*$	$\left(c d^{\xi^*}\right)^{r^*}$	✓	✓
g^{r^*}	$h^{r^*} \cdot M_b^*$	$u^{*\,a+\xi^* a'} \cdot (e^* / M_b^*)^{b+\xi^* b'}$	✓	✓

correctness of v

Security Proof

Check $c_i = (u_i, e_i, v_i)$ is an encryption of M_i:

$$M_i \stackrel{?}{=} e_i / u_i^s \quad (1) \qquad v_i \stackrel{?}{=} u_i^{a+\xi_i a'} \cdot (e_i / M_i)^{b+\xi_i b'} \quad (2)$$

Challenge:

$$c^* = (u^*, e^*, v^*) = \left(g^{r^*},\ h^{r^*} \cdot M_b^*,\ (c d^{\xi^*})^{r^*} \right) \quad \text{with } \xi^* = H(u^*, e^*).$$

c^*			Check		
u^*	e^*	v^*	(1)	(2)	
g^{r^*}	$h^{r^*} \cdot M_b^*$	$(c d^{\xi^*})^{r^*}$	✓	✓	
g^{r^*}	$h^{r^*} \cdot M_b^*$	$u^{*a+\xi^* a'} \cdot (e^*/M_b^*)^{b+\xi^* b'}$	✓	✓	correctness of v
g^{r^*}	$h^{r^*} \cdot M_b^*$	$u^{*a+\xi^* a'} \cdot (e^*/M_b^*)^{b+\xi^* b'}$		✓	2-universality of v

Security Proof

Check $c_i = (u_i, e_i, v_i)$ is an encryption of M_i:

$$M_i \stackrel{?}{=} e_i / u_i^s \quad (1) \qquad v_i \stackrel{?}{=} u_i^{a+\xi_i a'} \cdot (e_i / M_i)^{b+\xi_i b'} \quad (2)$$

Challenge:

$$c^* = (u^*, e^*, v^*) = \left(g^{r^*},\ h^{r^*} \cdot M_b^*,\ \left(c d^{\xi^*}\right)^{r^*} \right) \quad \text{with } \xi^* = H(u^*, e^*).$$

c^*			Check		
u^*	e^*	v^*	(1)	(2)	
g^{r^*}	$h^{r^*} \cdot M_b^*$	$\left(c d^{\xi^*}\right)^{r^*}$	✓	✓	
g^{r^*}	$h^{r^*} \cdot M_b^*$	$u^{*a+\xi^* a'} \cdot (e^*/M_b^*)^{b+\xi^* b'}$	✓	✓	correctness of v
g^{r^*}	$h^{r^*} \cdot M_b^*$	$u^{*a+\xi^* a'} \cdot (e^*/M_b^*)^{b+\xi^* b'}$		✓	2-universality of v
\$	\$	$u^{*a+\xi^* a'} \cdot (e^*/M_b^*)^{b+\xi^* b'}$		✓	DDH

Security Proof

Check $c_i = (u_i, e_i, v_i)$ is an encryption of M_i:

$$M_i \stackrel{?}{=} e_i / u_i^s \quad (1) \qquad v_i \stackrel{?}{=} u_i^{a+\xi_i a'} \cdot (e_i/M_i)^{b+\xi_i b'} \quad (2)$$

Challenge:

$$c^* = (u^*, e^*, v^*) = \left(g^{r^*},\ h^{r^*} \cdot M_b^*,\ (cd^{\xi^*})^{r^*}\right) \quad \text{with } \xi^* = H(u^*, e^*).$$

c^*			Check		
u^*	e^*	v^*	(1)	(2)	
g^{r^*}	$h^{r^*} \cdot M_b^*$	$(cd^{\xi^*})^{r^*}$	✓	✓	
g^{r^*}	$h^{r^*} \cdot M_b^*$	$u^{*a+\xi^* a'} \cdot (e^*/M_b^*)^{b+\xi^* b'}$	✓	✓	correctness of v
g^{r^*}	$h^{r^*} \cdot M_b^*$	$u^{*a+\xi^* a'} \cdot (e^*/M_b^*)^{b+\xi^* b'}$		✓	2-universality of v
\$	\$	$u^{*a+\xi^* a'} \cdot (e^*/M_b^*)^{b+\xi^* b'}$		✓	DDH
\$	\$	$u^{*a+\xi^* a'} \cdot (e^*/M_b^*)^{b+\xi^* b'}$	✓	✓	2-universality of v

Security Proof

Check $c_i = (u_i, e_i, v_i)$ is an encryption of M_i:

$$M_i \stackrel{?}{=} e_i / u_i^s \quad (1) \qquad v_i \stackrel{?}{=} u_i^{a+\xi_i a'} \cdot (e_i/M_i)^{b+\xi_i b'} \quad (2)$$

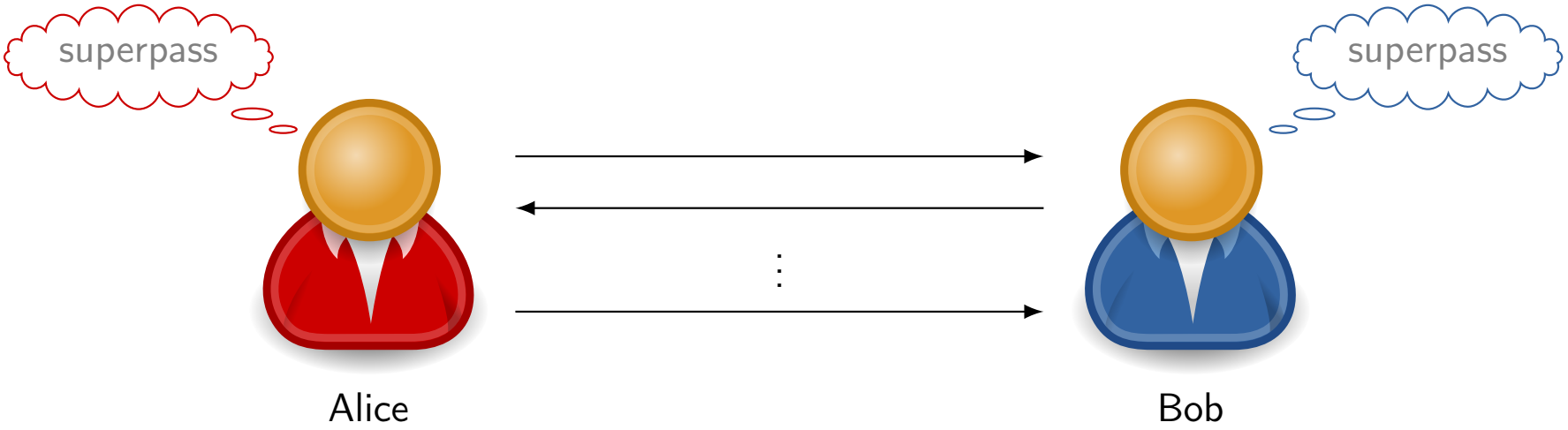
Challenge:

$$c^* = (u^*, e^*, v^*) = \left(g^{r^*},\ h^{r^*} \cdot M_b^*,\ (cd^{\xi^*})^{r^*}\right) \quad \text{with } \xi^* = H(u^*, e^*).$$

c^*			Check		
u^*	e^*	v^*	(1)	(2)	
g^{r^*}	$h^{r^*} \cdot M_b^*$	$(cd^{\xi^*})^{r^*}$	✓	✓	
g^{r^*}	$h^{r^*} \cdot M_b^*$	$u^{*a+\xi^* a'} \cdot (e^*/M_b^*)^{b+\xi^* b'}$	✓	✓	correctness of v
g^{r^*}	$h^{r^*} \cdot M_b^*$	$u^{*a+\xi^* a'} \cdot (e^*/M_b^*)^{b+\xi^* b'}$		✓	2-universality of v
\$	\$	$u^{*a+\xi^* a'} \cdot (e^*/M_b^*)^{b+\xi^* b'}$		✓	DDH
\$	\$	$u^{*a+\xi^* a'} \cdot (e^*/M_b^*)^{b+\xi^* b'}$	✓	✓	2-universality of v
\$	\$	\$	✓	✓	2-universality of v

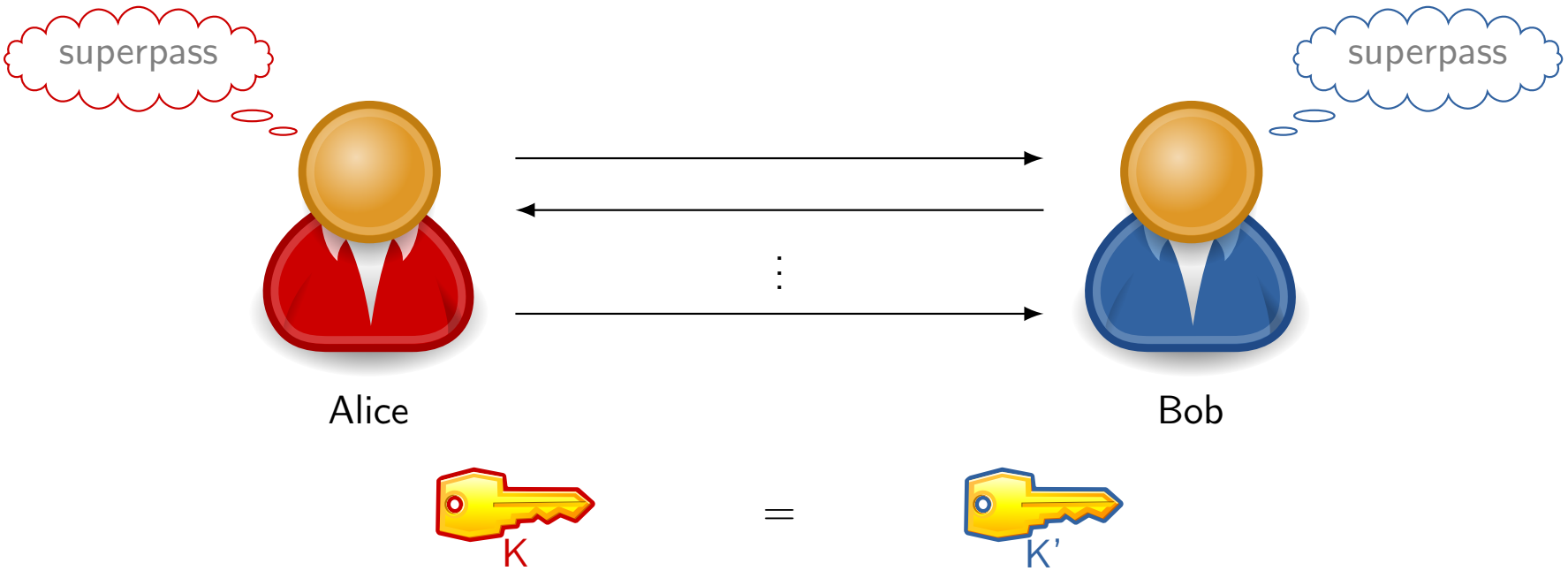
PAKE: Password-Authenticated Key Exchange

Goal: establishing a common secret key
from only a common low-entropy password



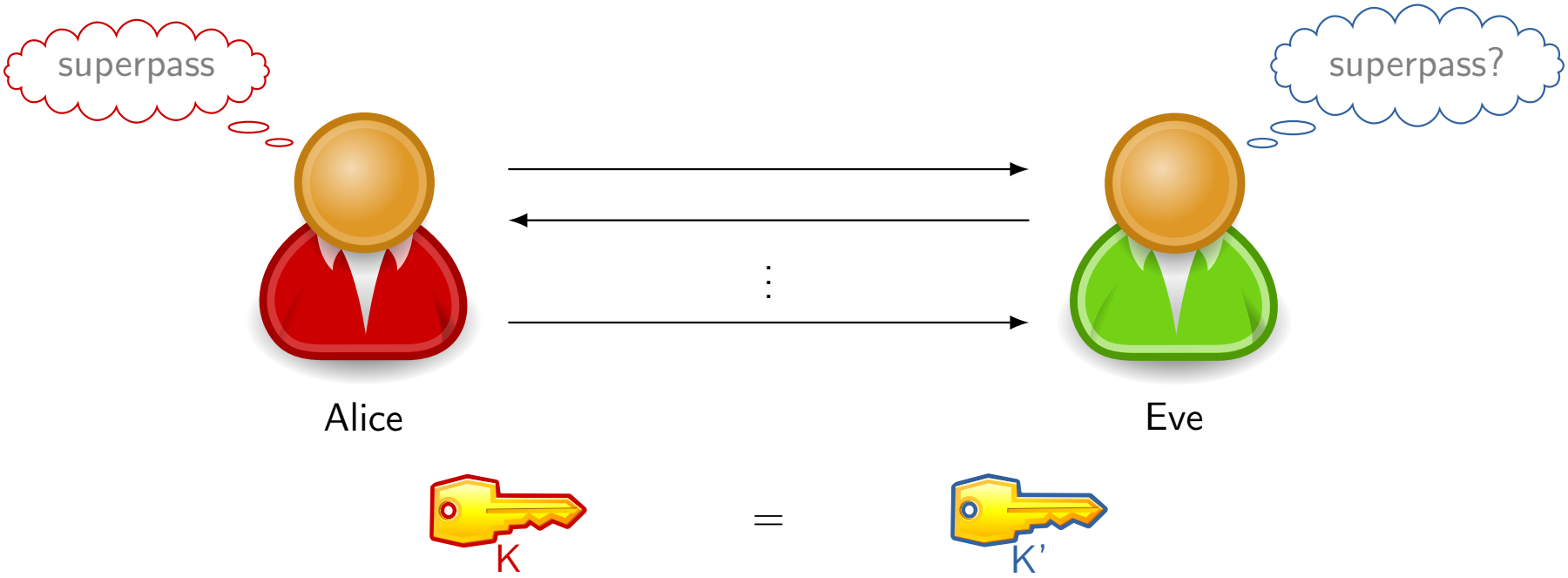
PAKE: Password-Authenticated Key Exchange

Goal: establishing a common secret key
from only a common low-entropy password



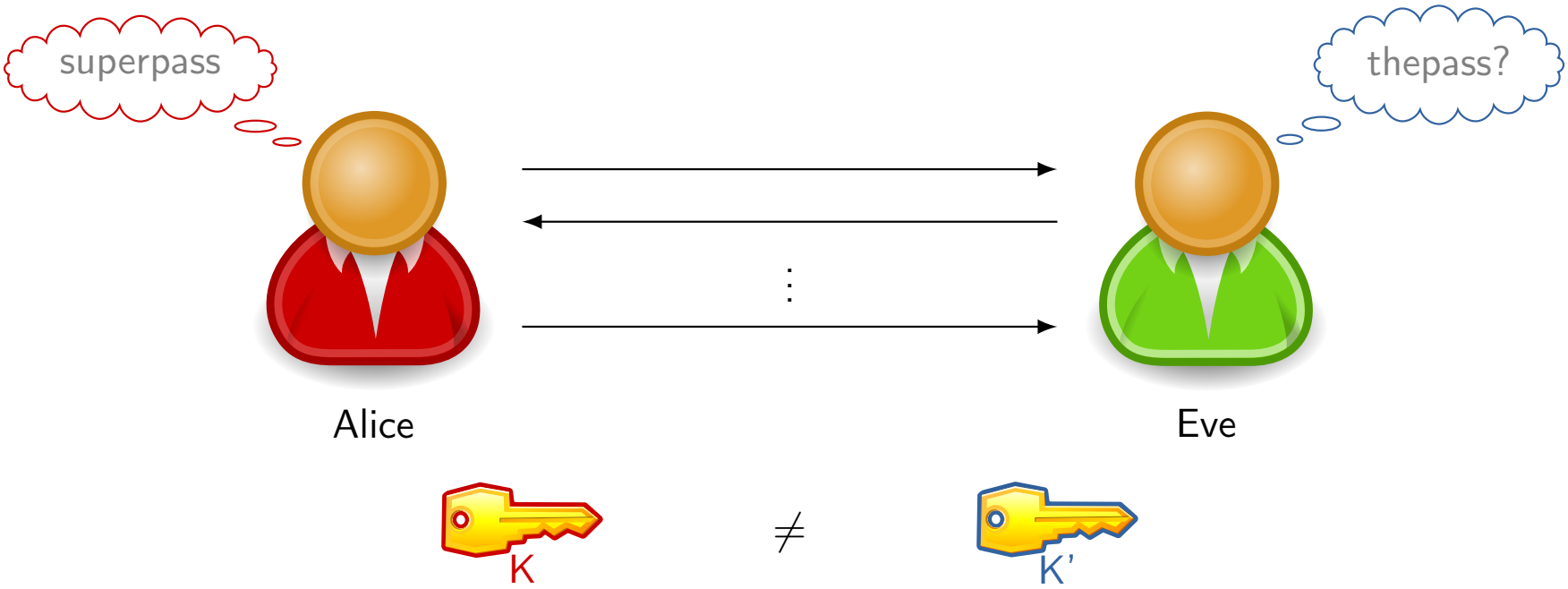
PAKE: Password-Authenticated Key Exchange

Goal: establishing a common secret key
from only a common low-entropy password



PAKE: Password-Authenticated Key Exchange

Goal: establishing a common secret key
from only a common low-entropy password

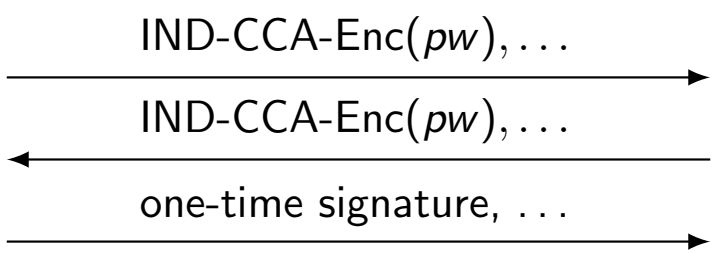


Intuitive security notion: only online dictionary attack works:

- at most one password can be tested per interaction;
- impossible to test password from an honest transcript.

PAKE Constructions from KOY/GL [KOY01, GL03] and JG/GK [JG04, GK10] Frameworks

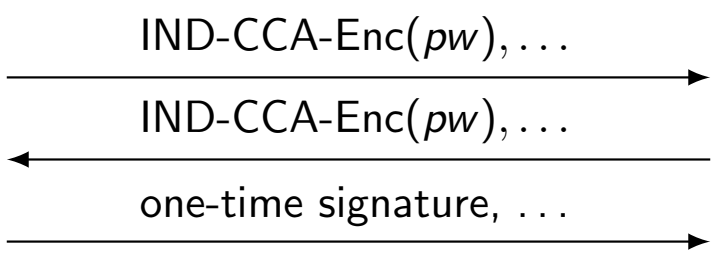
- Each user sends a ciphertext of his password pw;



KOY/GL

PAKE Constructions from KOY/GL [KOY01, GL03] and JG/GK [JG04, GK10] Frameworks

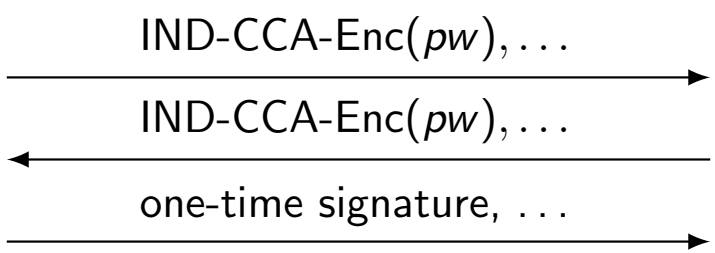
- Each user sends a ciphertext of his password pw;
- Small number of passwords $\longrightarrow$ IND-PCA sufficient;



KOY/GL

PAKE Constructions from KOY/GL [KOY01, GL03] and JG/GK [JG04, GK10] Frameworks

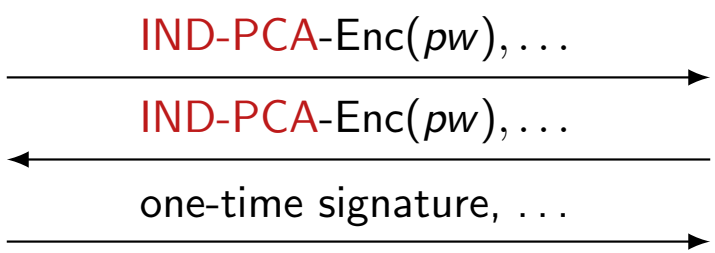
- Each user sends a ciphertext of his password pw;
- Small number of passwords $\longrightarrow$ IND-PCA sufficient;
  - ⚠ reduction loss = number of passwords;



KOY/GL

PAKE Constructions from KOY/GL [KOY01, GL03] and JG/GK [JG04, GK10] Frameworks

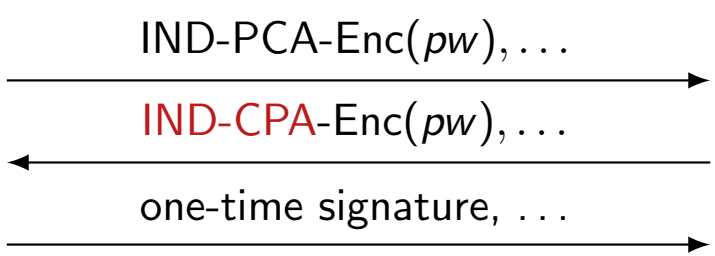
- Each user sends a ciphertext of his password pw;
- Small number of passwords $\longrightarrow$ IND-PCA sufficient;
  - ⚠ reduction loss = number of passwords;
- Here: direct proof with IND-PCA (in the model in [BPR00]);



KOY/GL

PAKE Constructions from KOY/GL [KOY01, GL03] and JG/GK [JG04, GK10] Frameworks

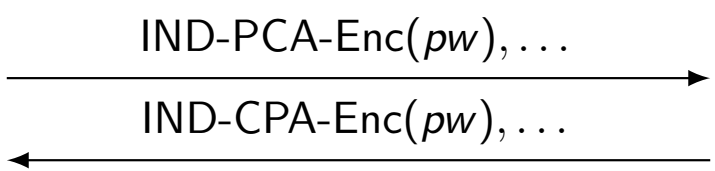
- Each user sends a ciphertext of his password pw;
- Small number of passwords $\longrightarrow$ IND-PCA sufficient;
  - ⚠ reduction loss = number of passwords;
- Here: direct proof with IND-PCA (in the model in [BPR00]);
  - \+ for KOY/GL, bonus can be applied:
    1 IND-CCA/PCA $\rightarrow$ 1 IND-CPA,



KOY/GL

PAKE Constructions from KOY/GL [KOY01, GL03] and JG/GK [JG04, GK10] Frameworks

- Each user sends a ciphertext of his password pw;
- Small number of passwords $\longrightarrow$ IND-PCA sufficient;
  - ⚠ reduction loss = number of passwords;
- Here: direct proof with IND-PCA (in the model in [BPR00]);
  - \+ for KOY/GL, bonus can be applied:
    1 IND-CCA/PCA $\rightarrow$ 1 IND-CPA, $\Rightarrow$ remove 1 round + 1 sig.



KOY/GL

Diffie-Hellman Based PAKE Constructions (BPR model)

	R / F	Assumptions		Complexity: Com.	Complexity: Time
EKE [BM92, BPR00]	1 / 2	ICM	CDH	$2 \times G$	4 exp
SPAKE2 [AP05]	1 / 2	ROM	CDH	$2 \times G$	4 exp
GK [JG04, GK10]	3 / 3	CRS	$\text{DDH}_{+\text{PRG}}$	$7 \times G$	18 exp
GL [KOY01, GL03]	3 / 3	CRS	DDH	$\approx 10 \times G$	27 exp
KV [KV11, BBC+13]	1 / 2	CRS	DDH	$12 \times G$	34 exp
GK-SPOKE	2 / 2	CRS	$\text{DDH}_{+\text{PRG}}$	$6 \times G$	17 exp
GL-SPOKE	2 / 2	CRS	DDH	$7 \times G$	21 exp
KV-SPOKE	1 / 2	CRS	DDH	$10 \times G$	30 exp

R: rounds, F: flows;
ICM: ideal-cipher model, ROM: random-oracle model
CRS: common reference string;
Variant of GK with Kurosawa-Desmedt [KD04, GS04] possible.

Thank you for your attention!

- New security notion: IND-PCA inspired from [OP01];
- New (algebraic) encryption scheme: Short Cramer-Shoup:

$$c = \left(u = g^r,\ e = h^r \cdot M,\ v = \left(cd^{\xi}\right)^r\right) \quad \text{with } \xi = H(u, e);$$

- Applications:
  - small messages/scalar/bit IND-CCA encryption;
  - PAKE from KOY / GL and GK frameworks;

Image credit: www.h3dwallpapers.com, www.terunanting.com, absurdwordpreferred.deviantart.com

References I

Michel Abdalla and David Pointcheval.

Simple password-based encrypted key exchange protocols.

In Alfred Menezes, editor, *CT-RSA 2005*, volume 3376 of *LNCS*, pages 191–208. Springer, February 2005.

Fabrice Benhamouda, Olivier Blazy, Céline Chevalier, David Pointcheval, and Damien Vergnaud.

New techniques for SPHFs and efficient one-round PAKE protocols.

In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 449–475. Springer, August 2013.

Steven M. Bellovin and Michael Merritt.

Encrypted key exchange: Password-based protocols secure against dictionary attacks.

In *1992 IEEE Symposium on Security and Privacy*, pages 72–84. IEEE Computer Society Press, May 1992.

References II

Mihir Bellare, David Pointcheval, and Phillip Rogaway.

Authenticated key exchange secure against dictionary attacks.

In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 139–155. Springer, May 2000.

Olivier Blazy, David Pointcheval, and Damien Vergnaud.

Round-optimal privacy-preserving protocols with smooth projective hash functions.

In Ronald Cramer, editor, *TCC 2012*, volume 7194 of *LNCS*, pages 94–111. Springer, March 2012.

Ronald Cramer and Victor Shoup.

Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption.

In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 45–64. Springer, April / May 2002.

References III

Adam Groce and Jonathan Katz.

A new framework for efficient password-based authenticated key exchange.

In Ehab Al-Shaer, Angelos D. Keromytis, and Vitaly Shmatikov, editors, *ACM CCS 10*, pages 516–525. ACM Press, October 2010.

Rosario Gennaro and Yehuda Lindell.

A framework for password-based authenticated key exchange.

In Eli Biham, editor, *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 524–543. Springer, May 2003.

`http://eprint.iacr.org/2003/032.ps.gz`.

References IV

Rosario Gennaro and Victor Shoup.

A note on an encryption scheme of kurosawa and desmedt.

Cryptology ePrint Archive, Report 2004/194, 2004.

http://eprint.iacr.org/2004/194.

Jens Groth and Amit Sahai.

Efficient non-interactive proof systems for bilinear groups.

In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432. Springer, April 2008.

Shaoquan Jiang and Guang Gong.

Password based key exchange with mutual authentication.

In Helena Handschuh and Anwar Hasan, editors, *SAC 2004*, volume 3357 of *LNCS*, pages 267–279. Springer, August 2004.

References V

Kaoru Kurosawa and Yvo Desmedt.

A new paradigm of hybrid encryption scheme.

In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 426–442. Springer, August 2004.

Jonathan Katz, Rafail Ostrovsky, and Moti Yung.

Efficient password-authenticated key exchange using human-memorable passwords.

In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 475–494. Springer, May 2001.

Jonathan Katz and Vinod Vaikuntanathan.

Round-optimal password-based authenticated key exchange.

In Yuval Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 293–310. Springer, March 2011.

References VI

Tatsuaki Okamoto and David Pointcheval.

REACT: Rapid Enhanced-security Asymmetric Cryptosystem Transform.

In David Naccache, editor, *CT-RSA 2001*, volume 2020 of *LNCS*, pages 159–175. Springer, April 2001.