Improved Strongly Deniable Authenticated Key Exchanges For Secure Messaging

Nik Unger

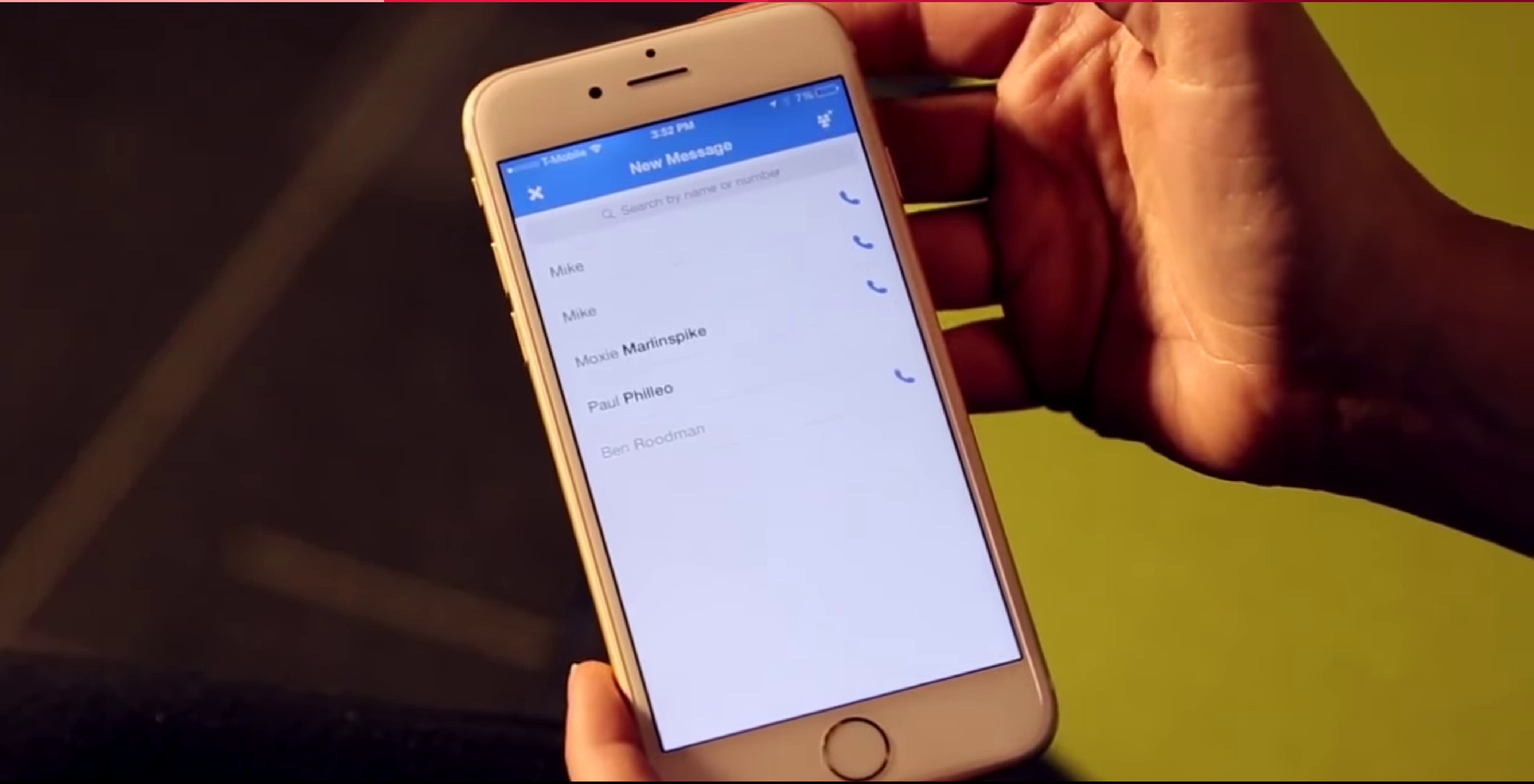
and

Ian Goldberg

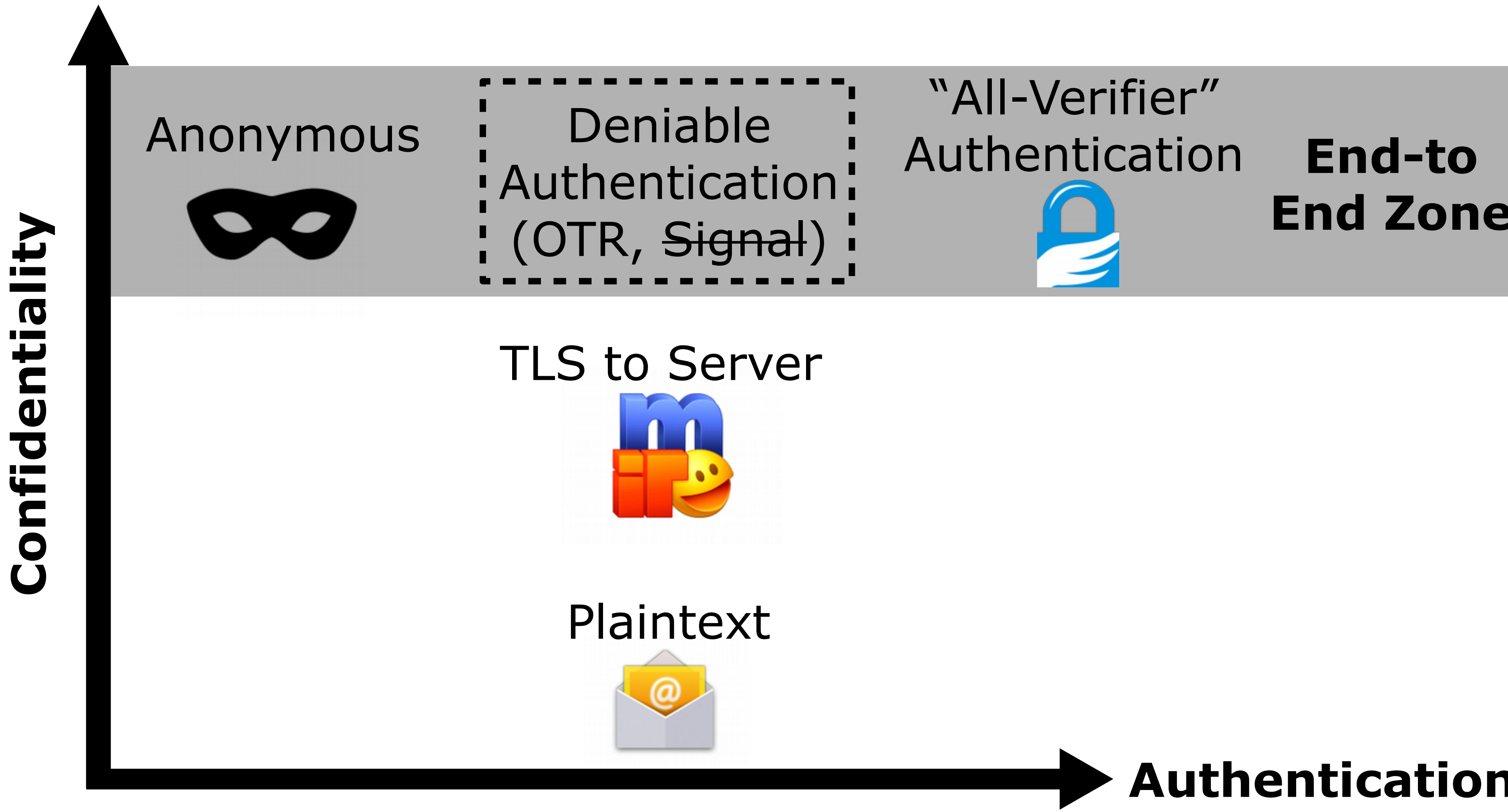
UNIVERSITY OF WATERLOO
FACULTY OF MATHEMATICS
David R. Cheriton School
of Computer Science

CrySP

Secure Messaging



Secure Messaging



Why Deniability?

HERE'S CRYPTOGRAPHIC PROOF THAT DONNA BRAZILE IS WRONG, WIKILEAKS EMAILS ARE REAL

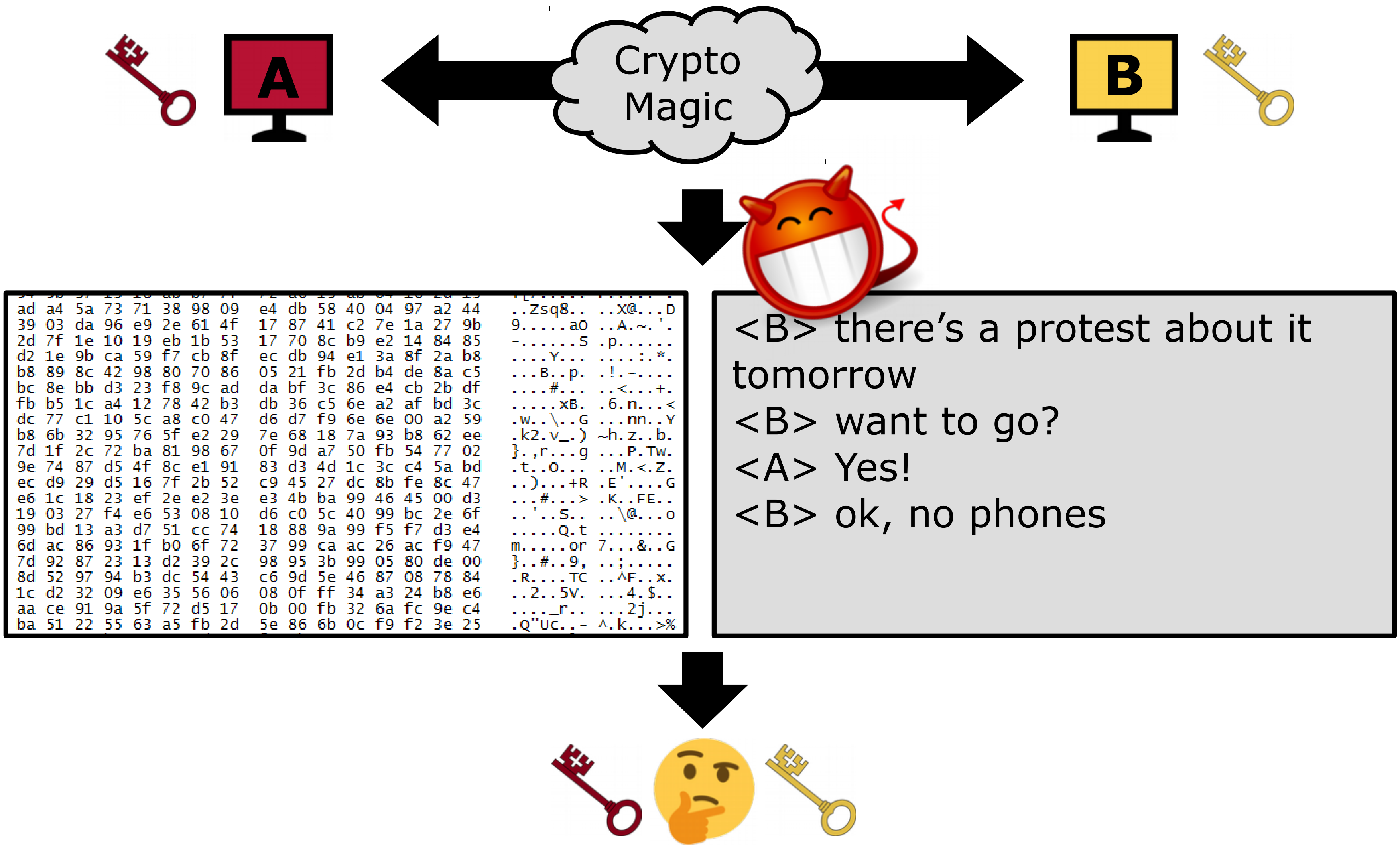
Luke Rosiak | Investigative Reporter **7:10 PM 10/21/2016**

Cryptographic signatures demonstrate that Democratic National Committee Chairman Donna Brazile is wrong when she suggests the WikiLeaks emails were altered and that she did not send an email tipping off Democratic presidential nominee Hillary Clinton to debate questions.

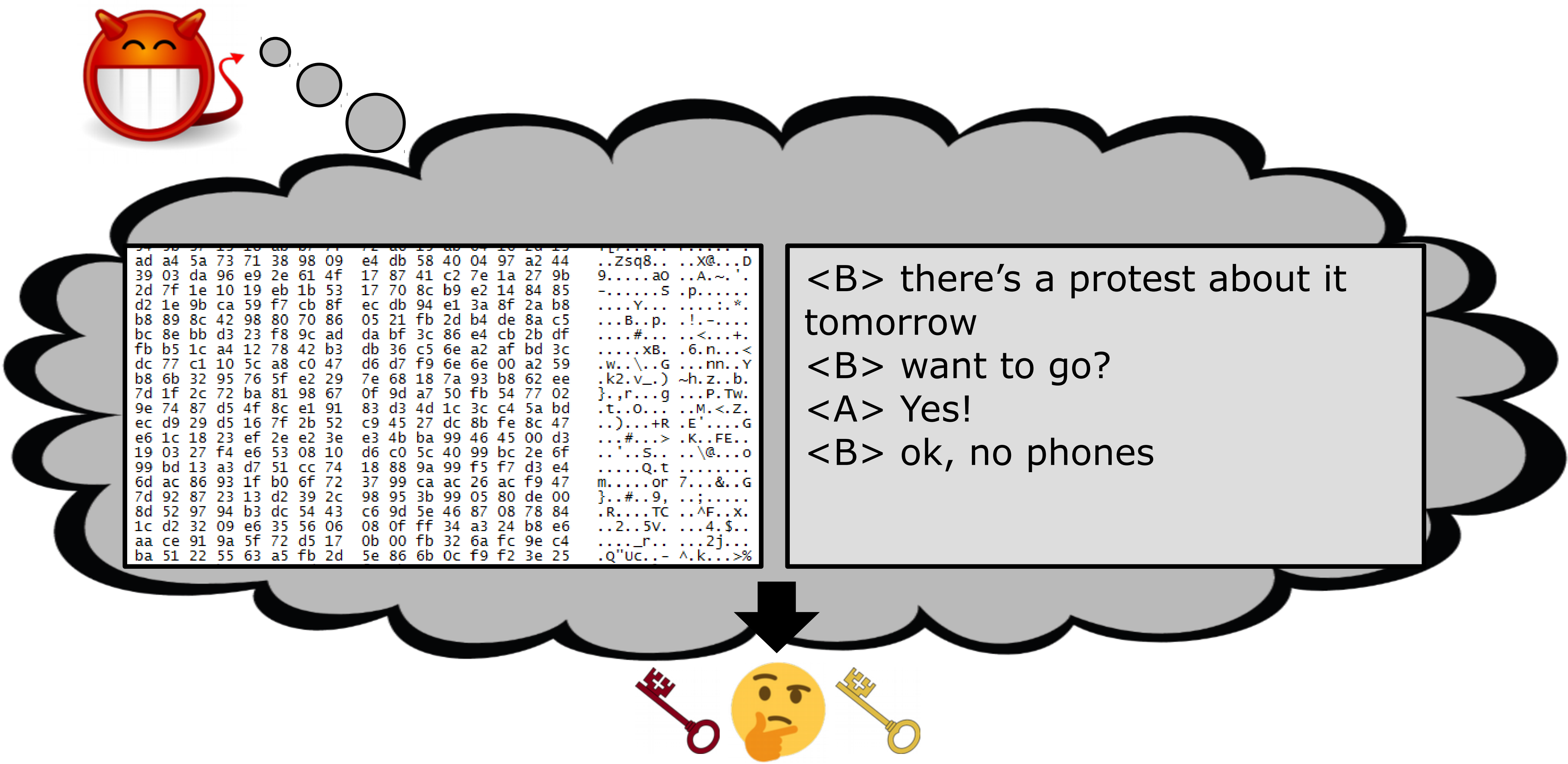
Many email systems use a verification system called DomainKeys Identified Mail (DKIM) that shows whether an email has been changed. It uses a key stored on the email server that sent the email, so it can't be forged.

HillaryClinton.com uses Gmail to handle its mail and uses DKIM. Staffer Jennifer Palmieri, using her HillaryClinton.com email, replied to a Brazile email warning that Brazile was "worried" about Clinton's ability to answer a question about the

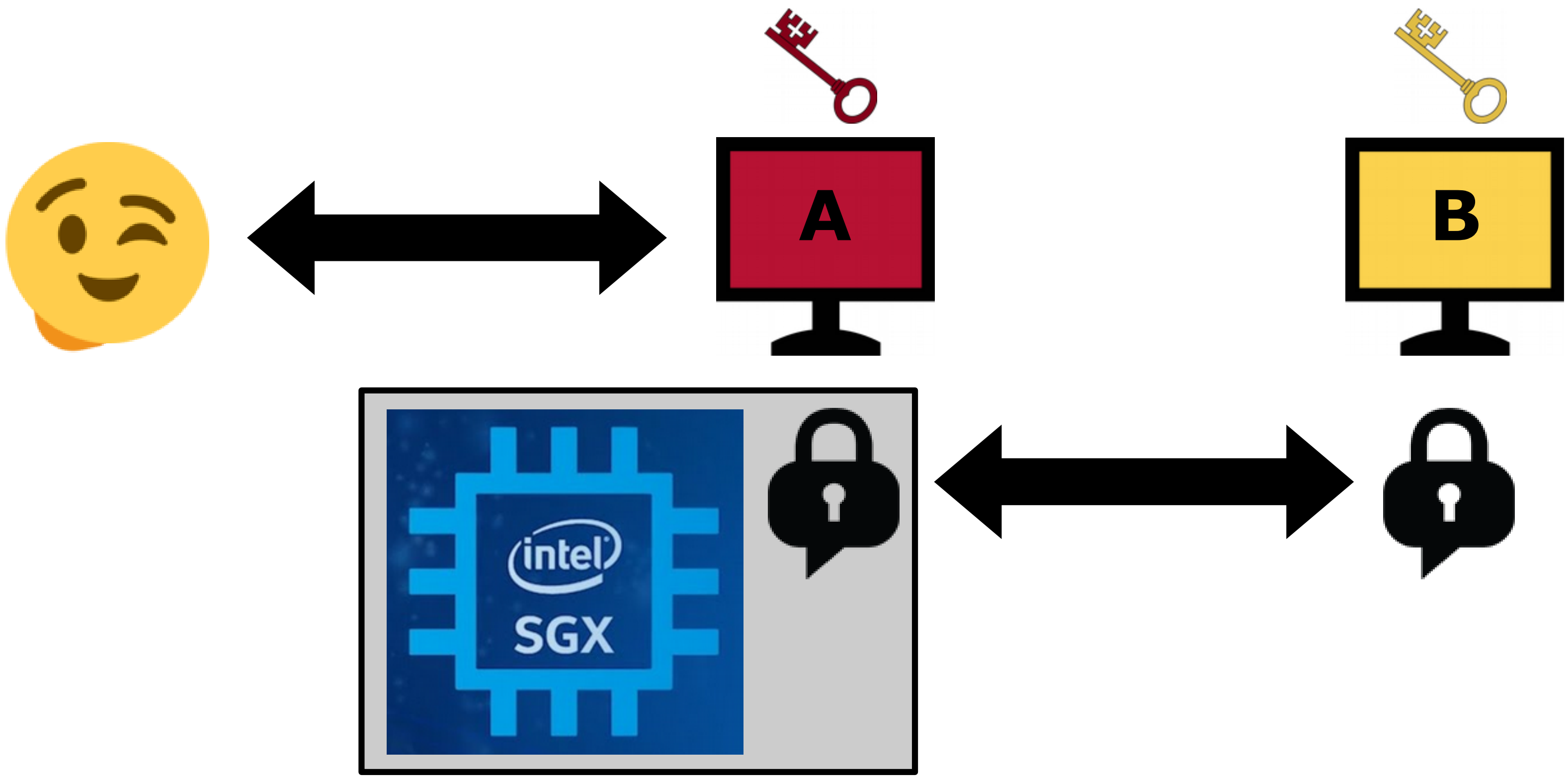
Deniable Messaging



Deniable Messaging

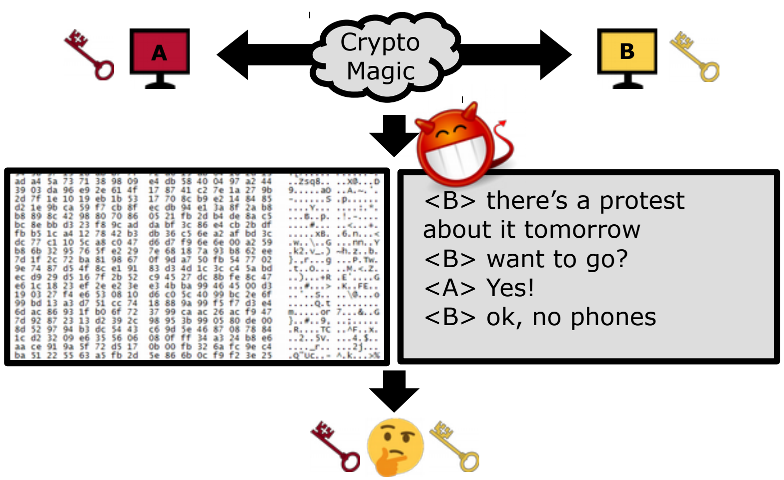


Deniable Messaging...?

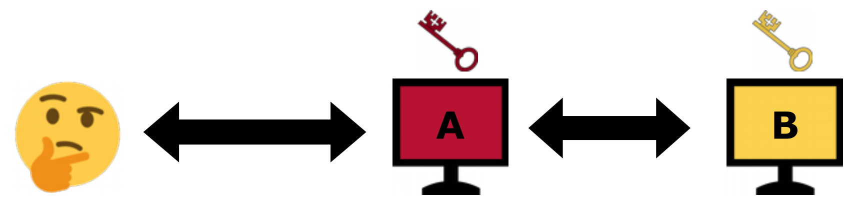


Offline vs. Online Deniability

Offline Deniability



Online Deniability



Deniable Messaging...?

- See Appendix A
  - Attacks on OTRv3 and Signal
- Also see ia.cr/2018/424:

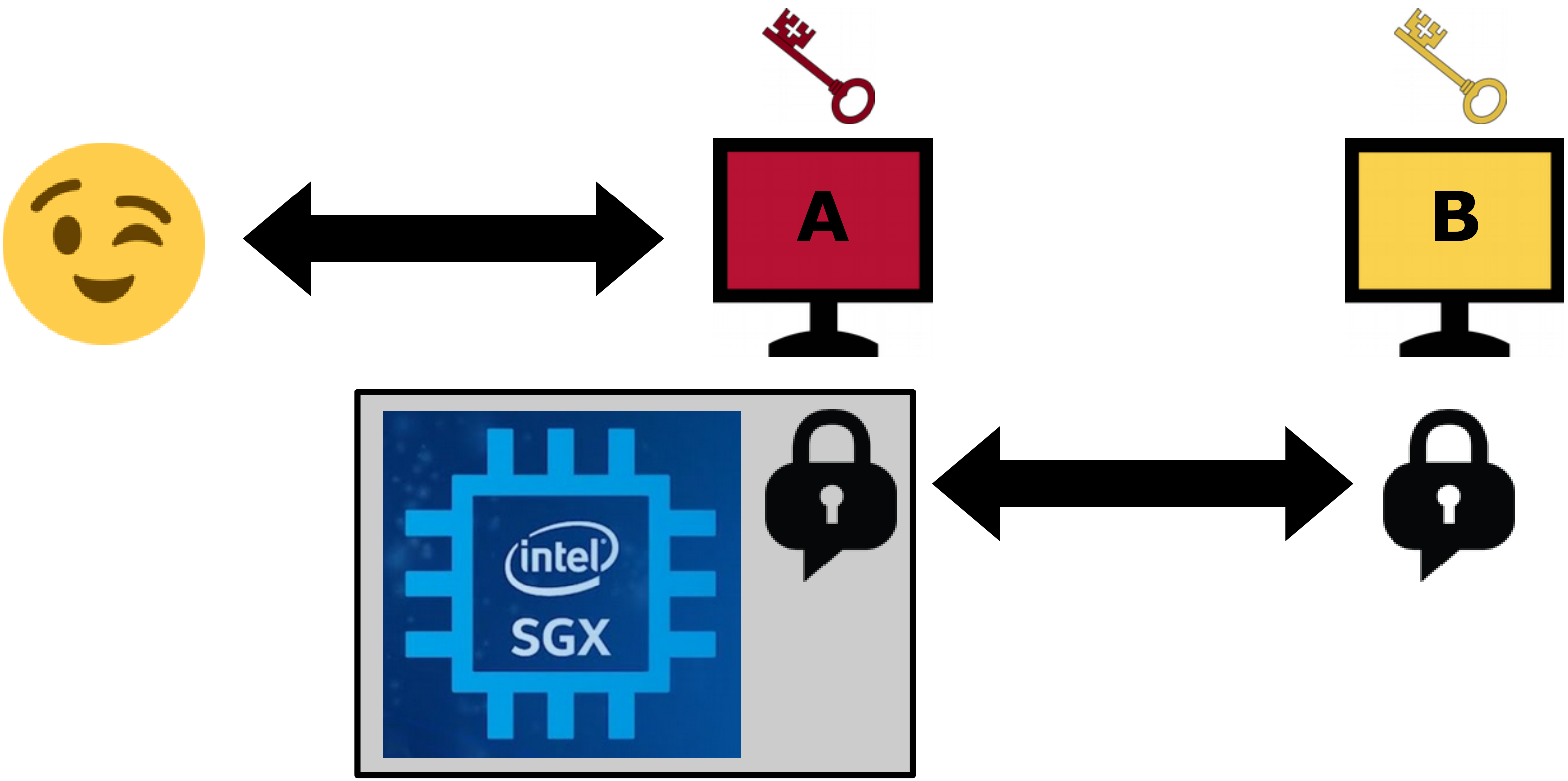
On The Use of Remote Attestation to Break and Repair Deniability

Lachlan J. Gunn
Aalto University
lachlan.gunn@aalto.fi

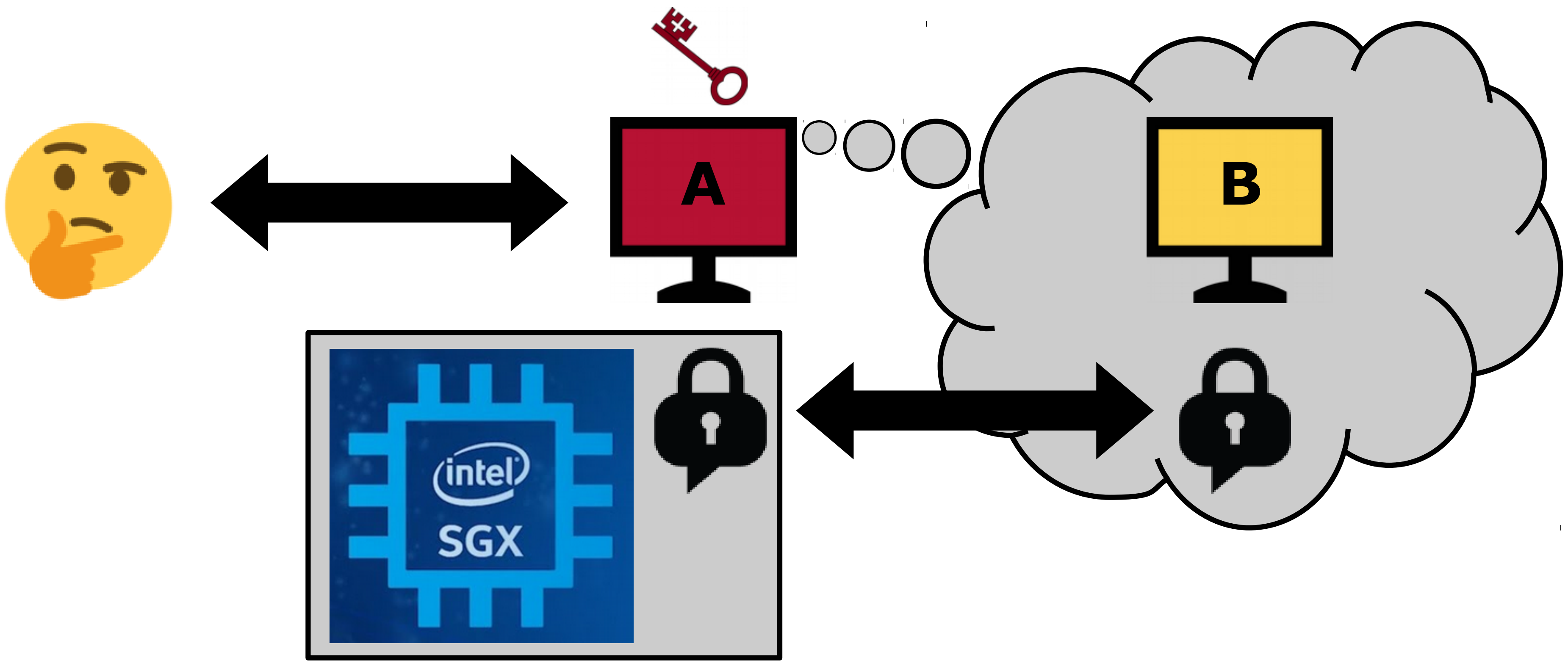
Ricardo Vieitez Parra
Aalto University
ricardo.vieitezparra@aalto.fi

N. Asokan
Aalto University
asokan@acm.org

Deniable Messaging

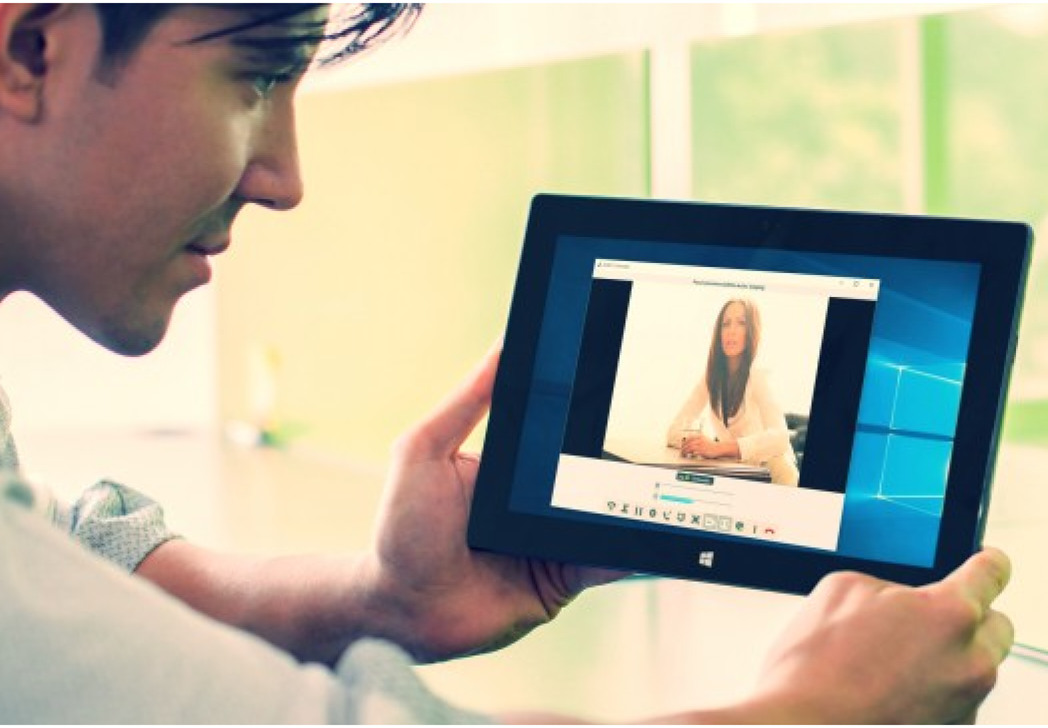


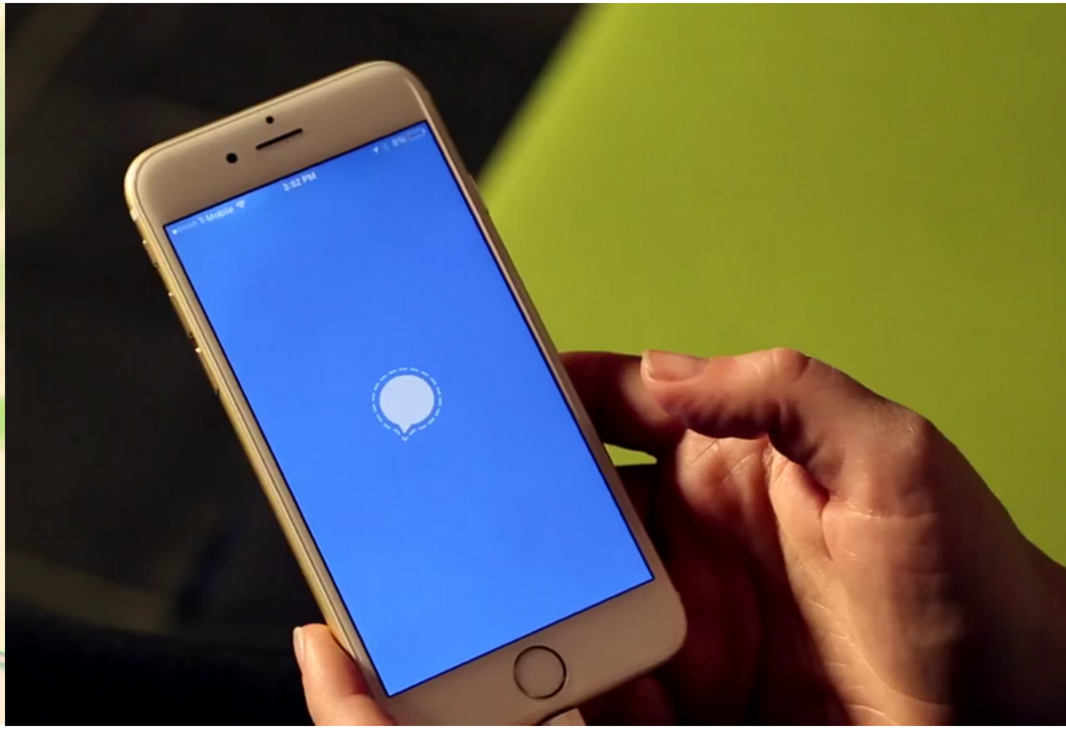
Deniable Messaging



In This Paper

- Two new efficient key exchange protocols





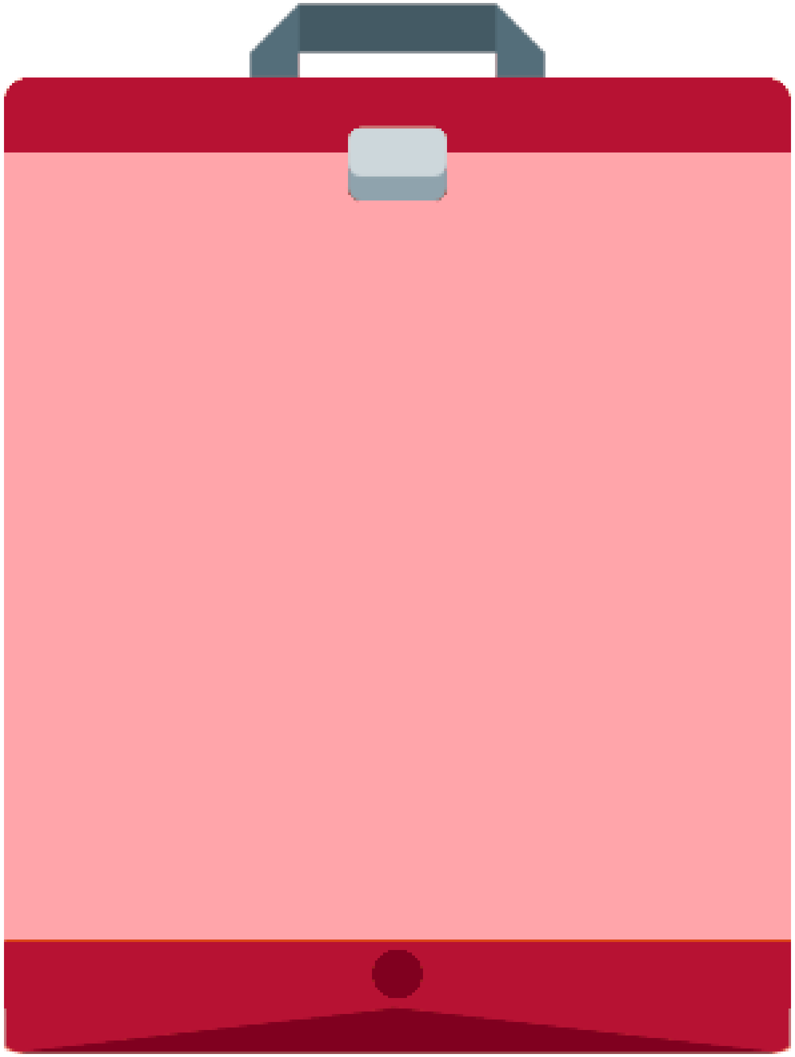
Interactive

Non-interactive

Security Properties

- Confidentiality
- Mutual authentication
- Forward secrecy
- Contributiveness
- Offline and online deniability

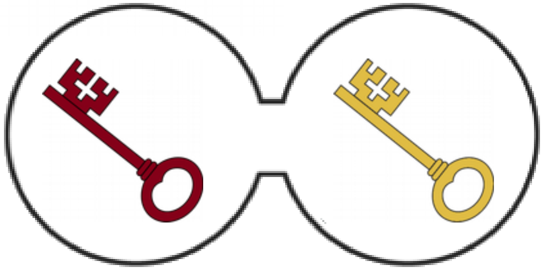
Crypto Toolbox



Identity key
(long-term asymmetric)

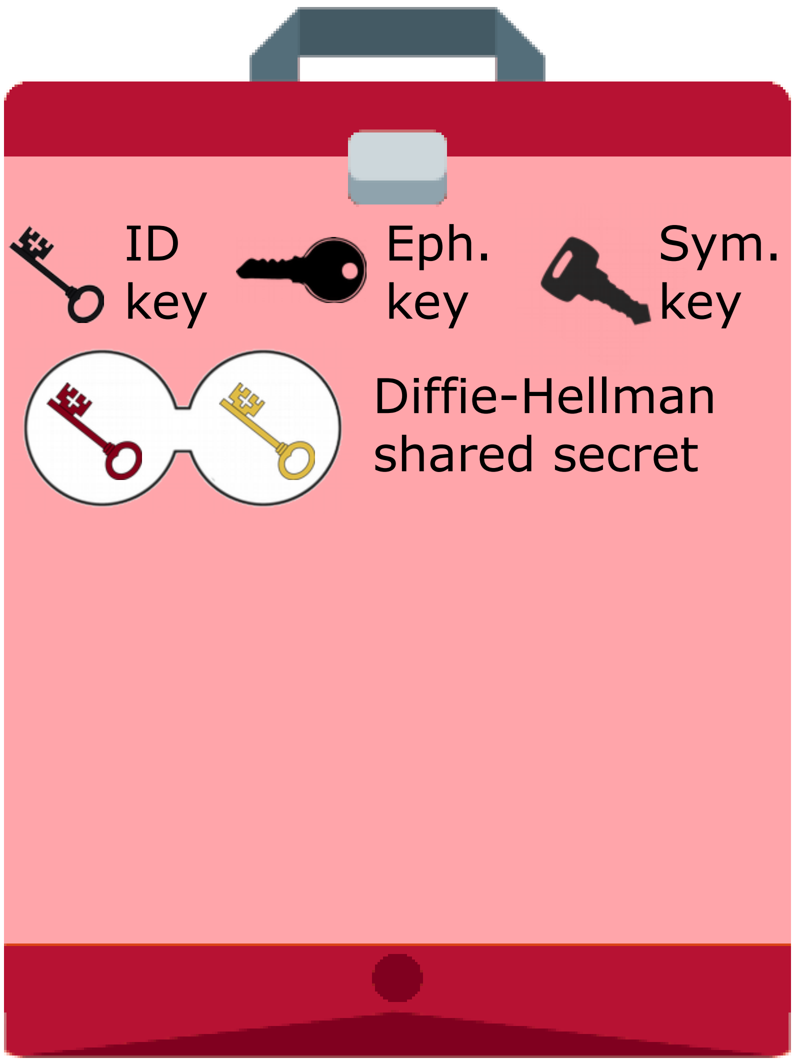
Ephemeral key
(short-term asymmetric)

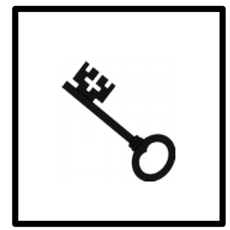
Shared session key
(symmetric)



Diffie-Hellman
shared secret

Crypto Toolbox



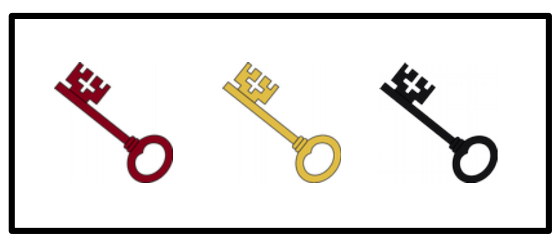


Signature

Create: need private
Verify: need public

MAC

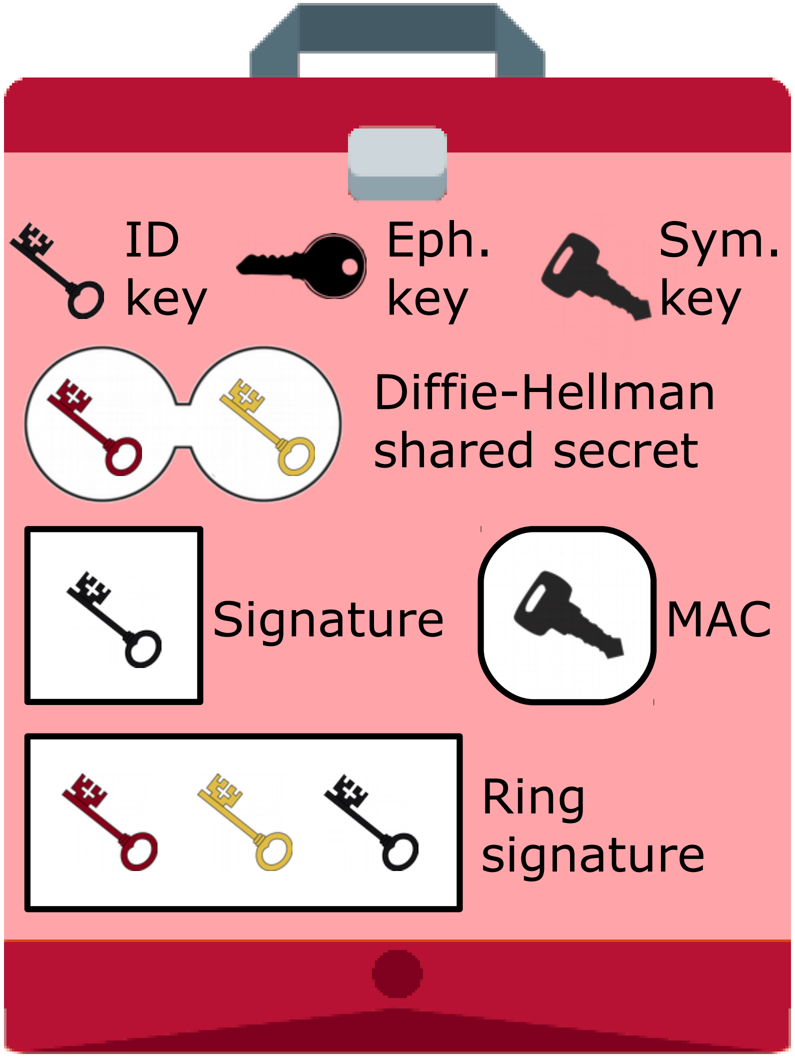
Create: need
Verify: need



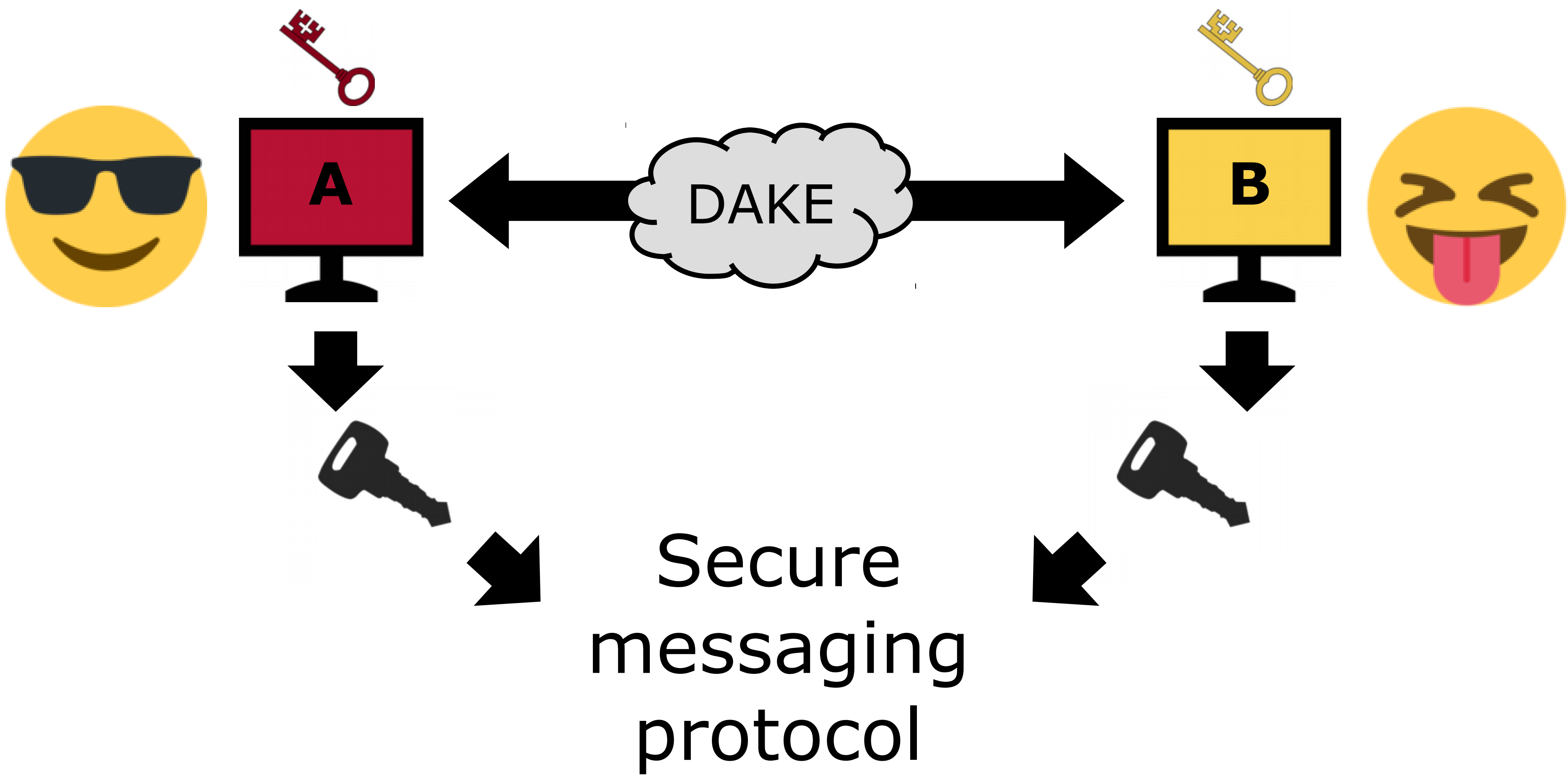
Ring signature

Create: need **one** private
, , or
Verify: need **all** public
, , and

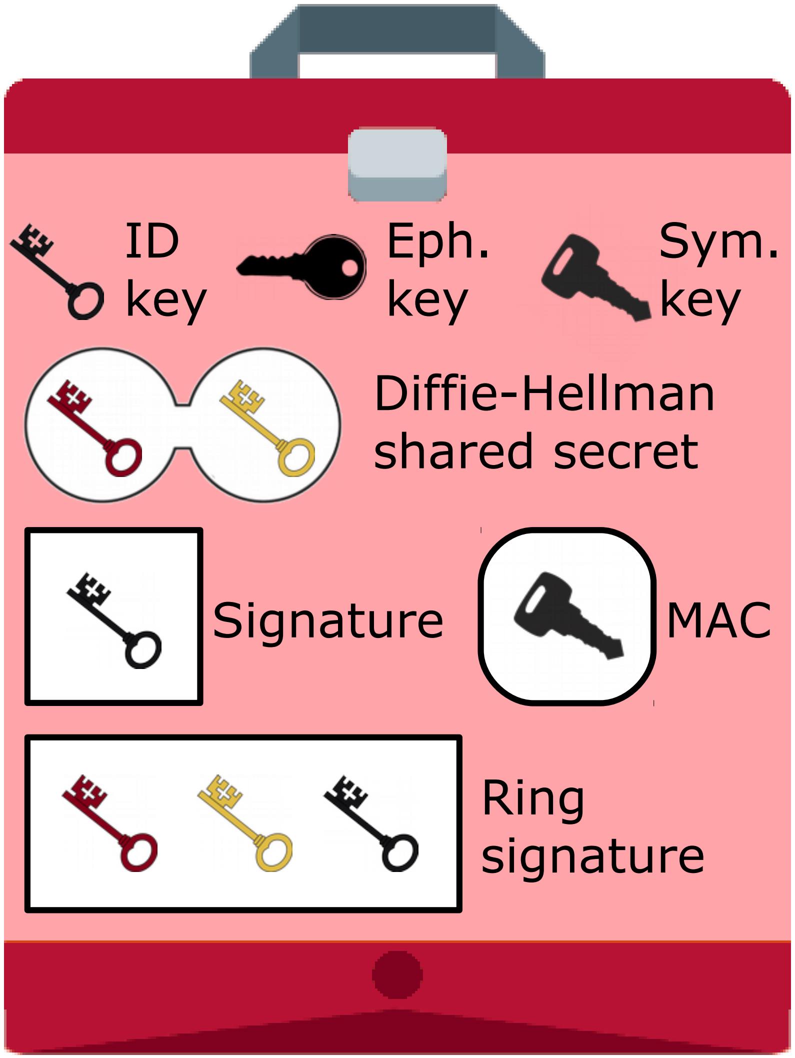
Crypto Toolbox

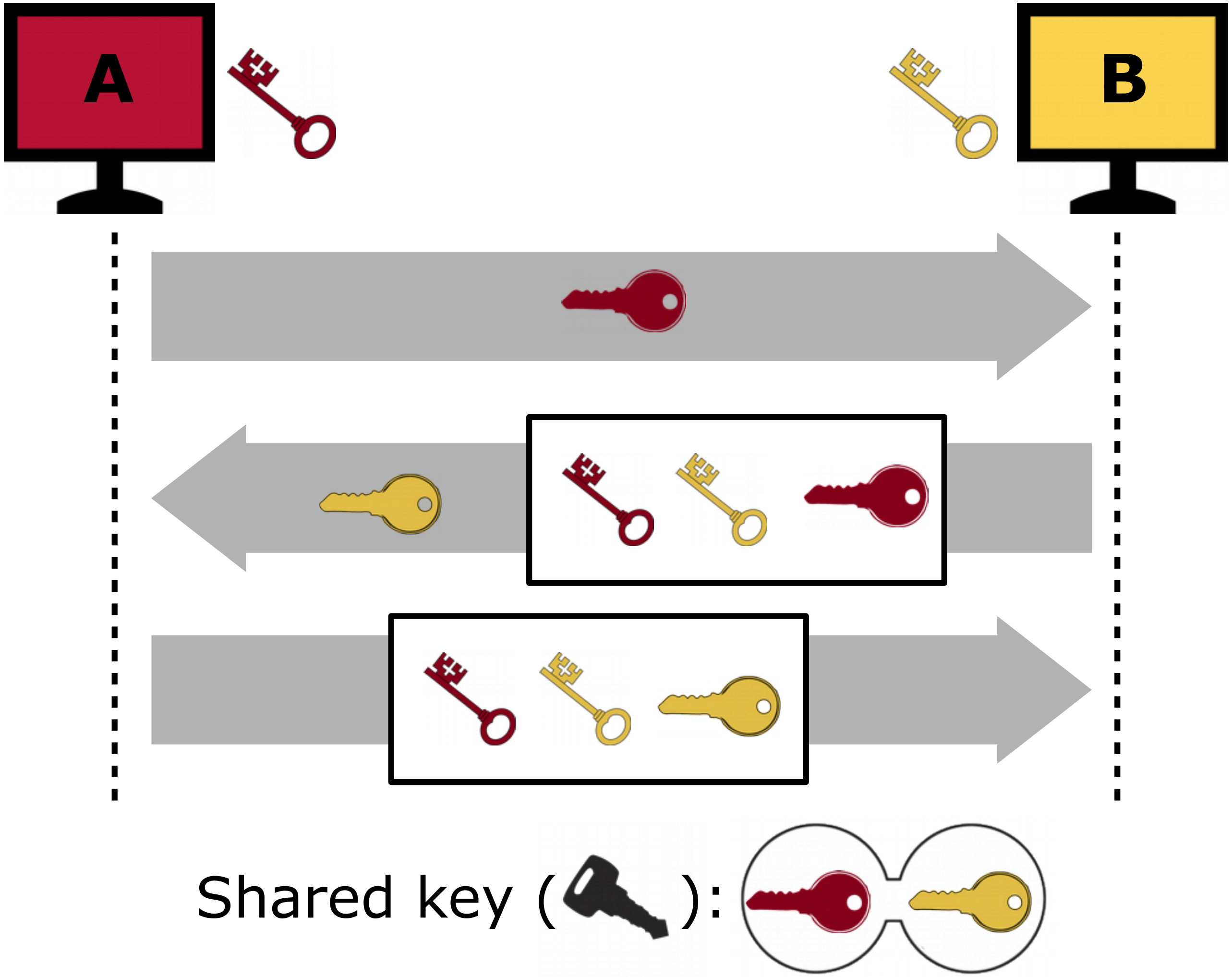


Deniable Authenticated Key Exchanges

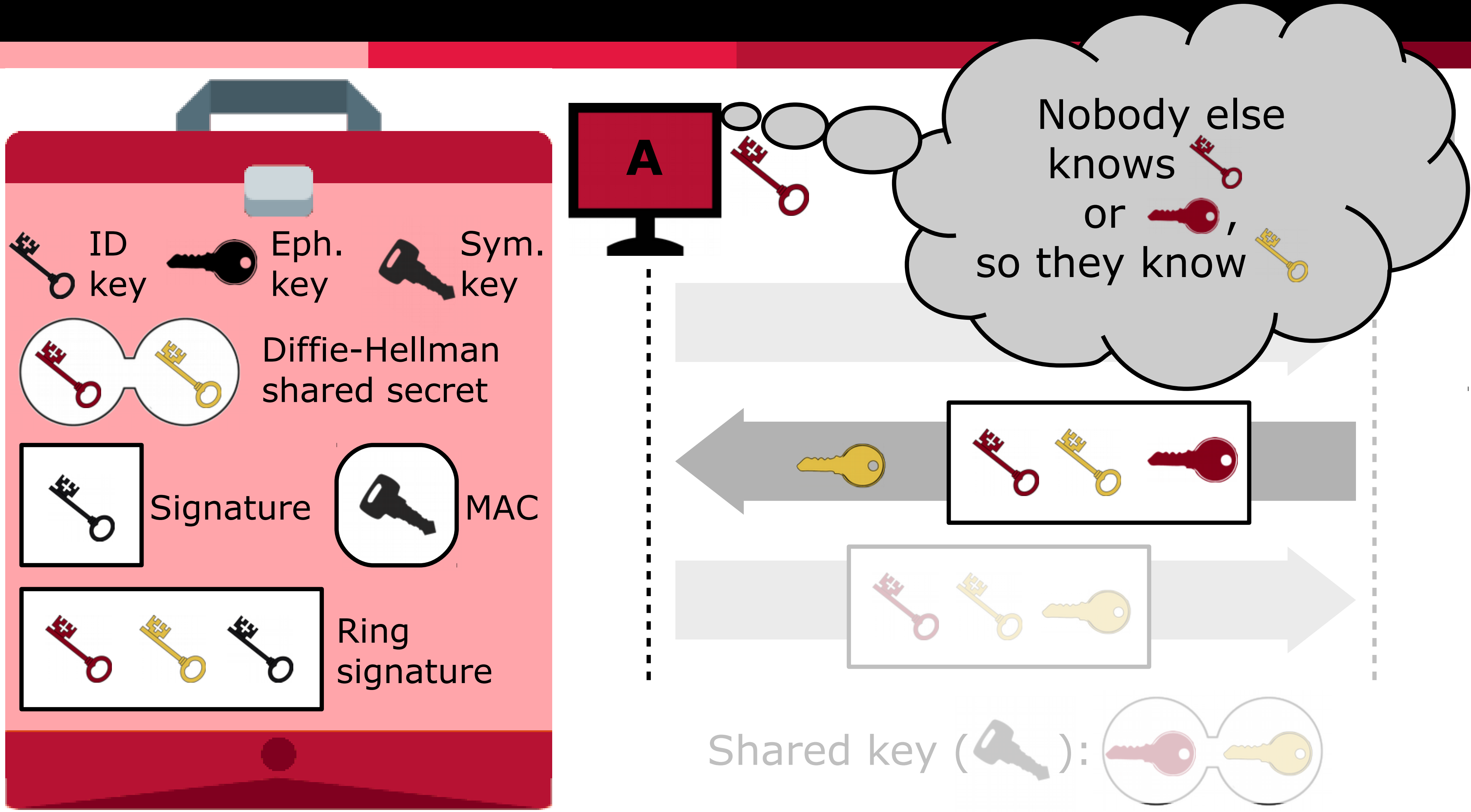


DAKEZ

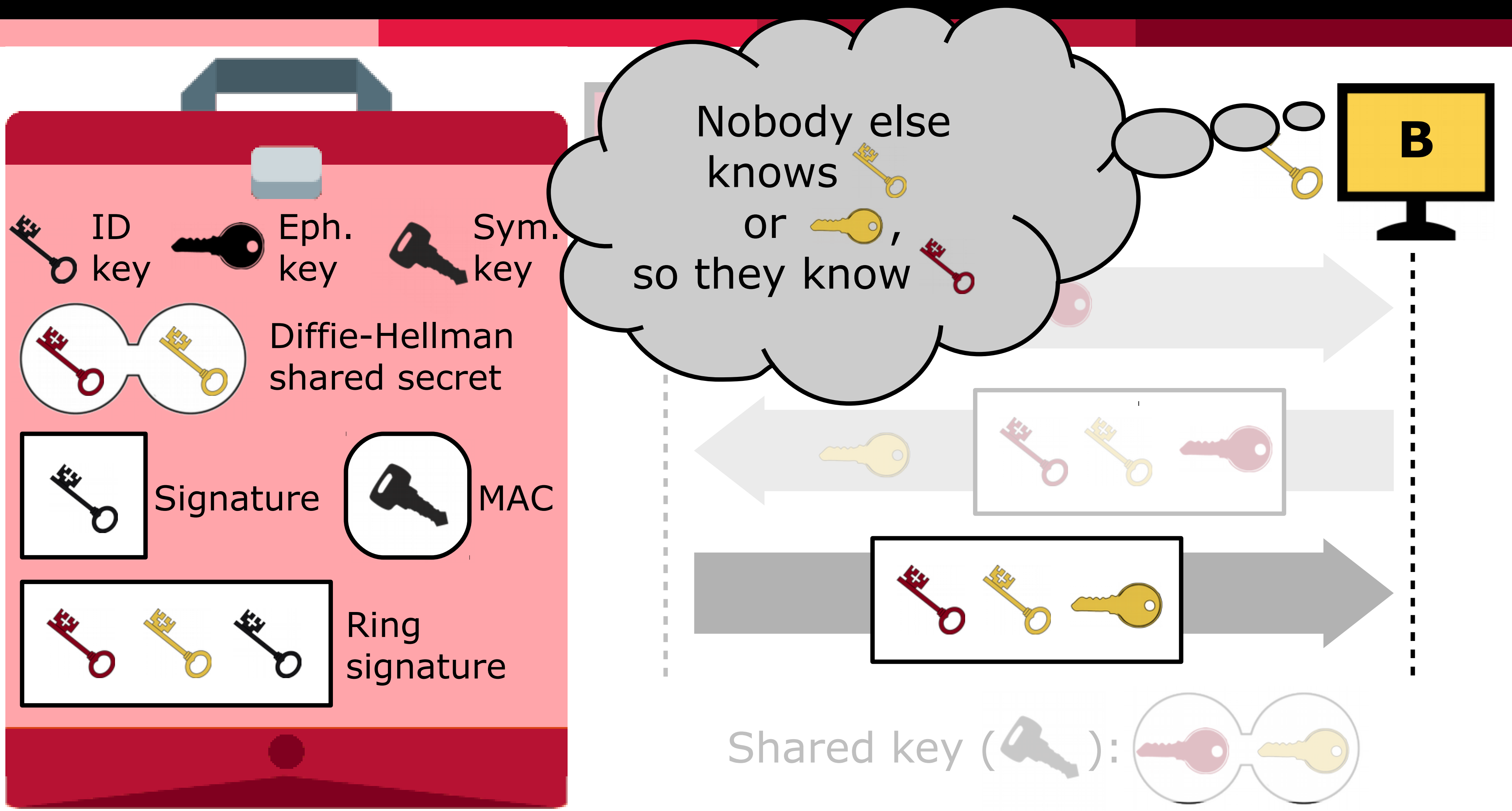

ID key
Eph. key
Sym. key
Diffie-Hellman shared secret
Signature
MAC
Ring signature


A
B
Shared key ( ):

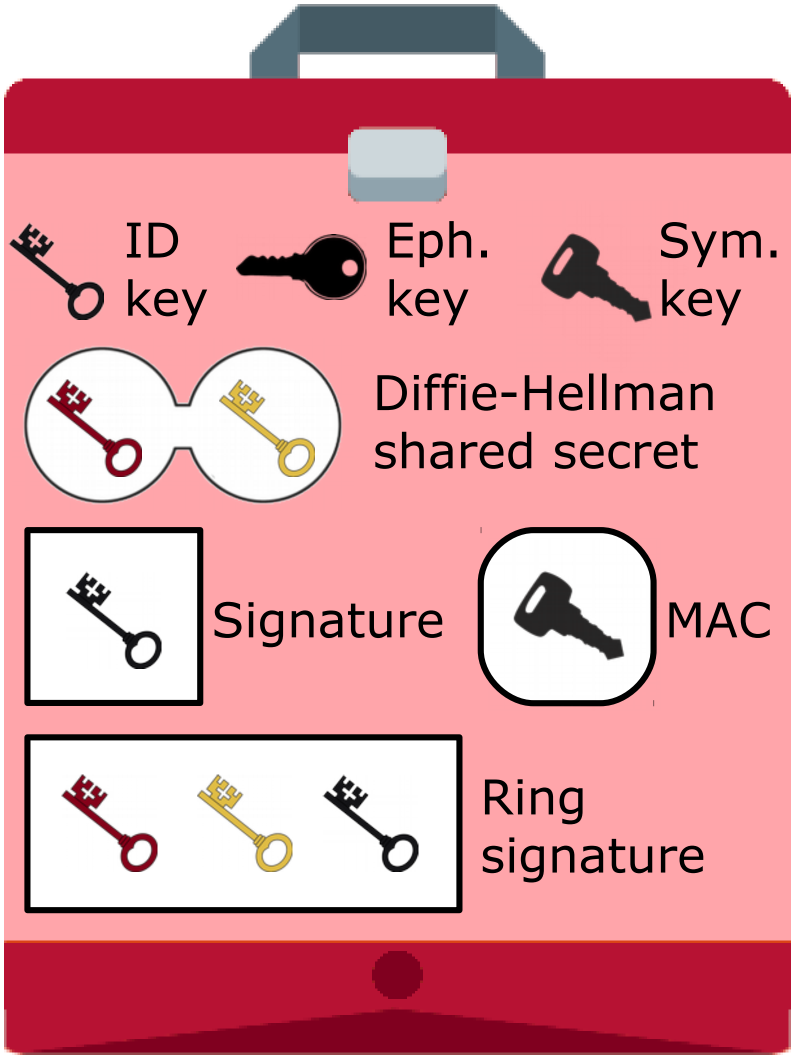
DAKEZ: Authentication

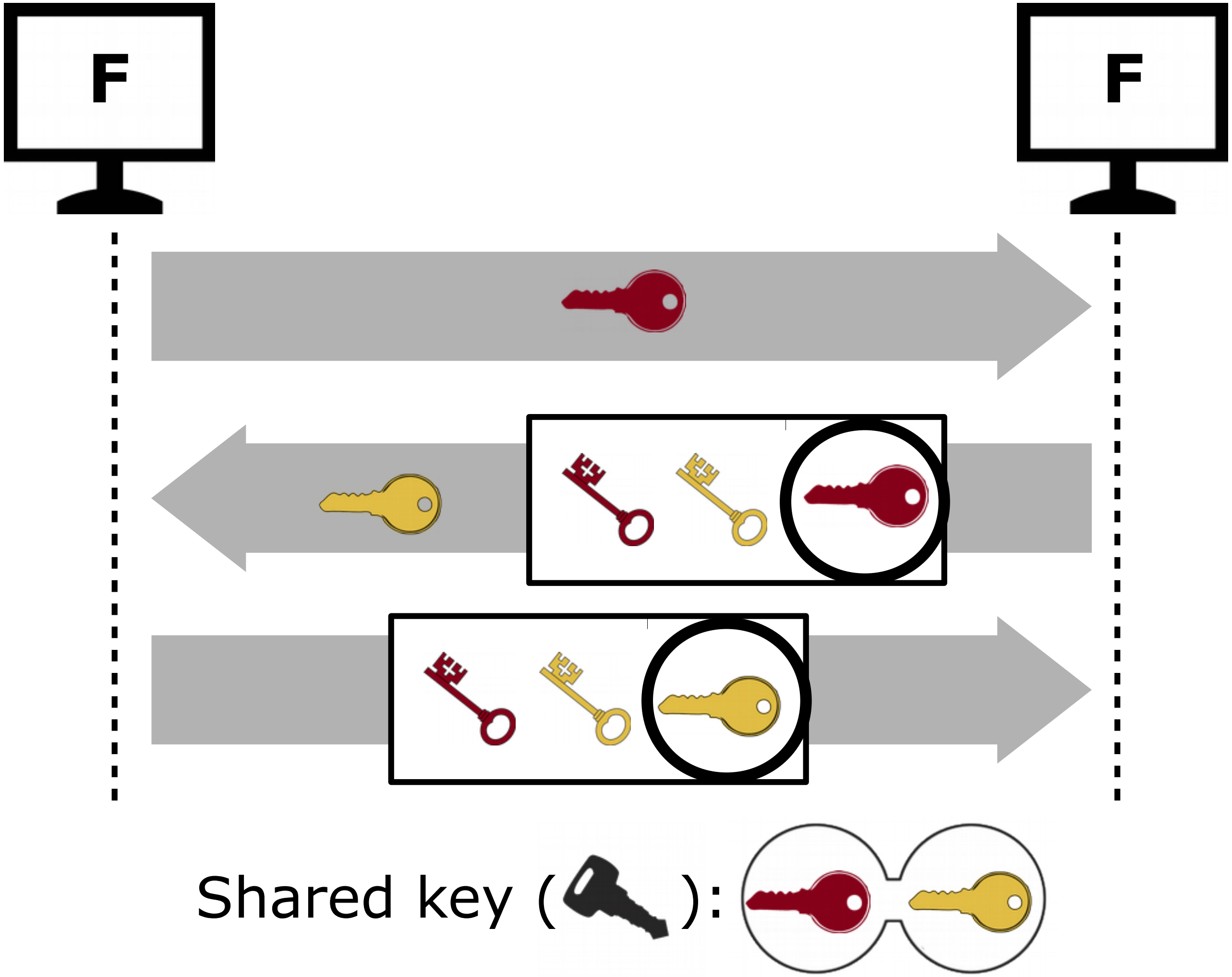


DAKEZ: Authentication

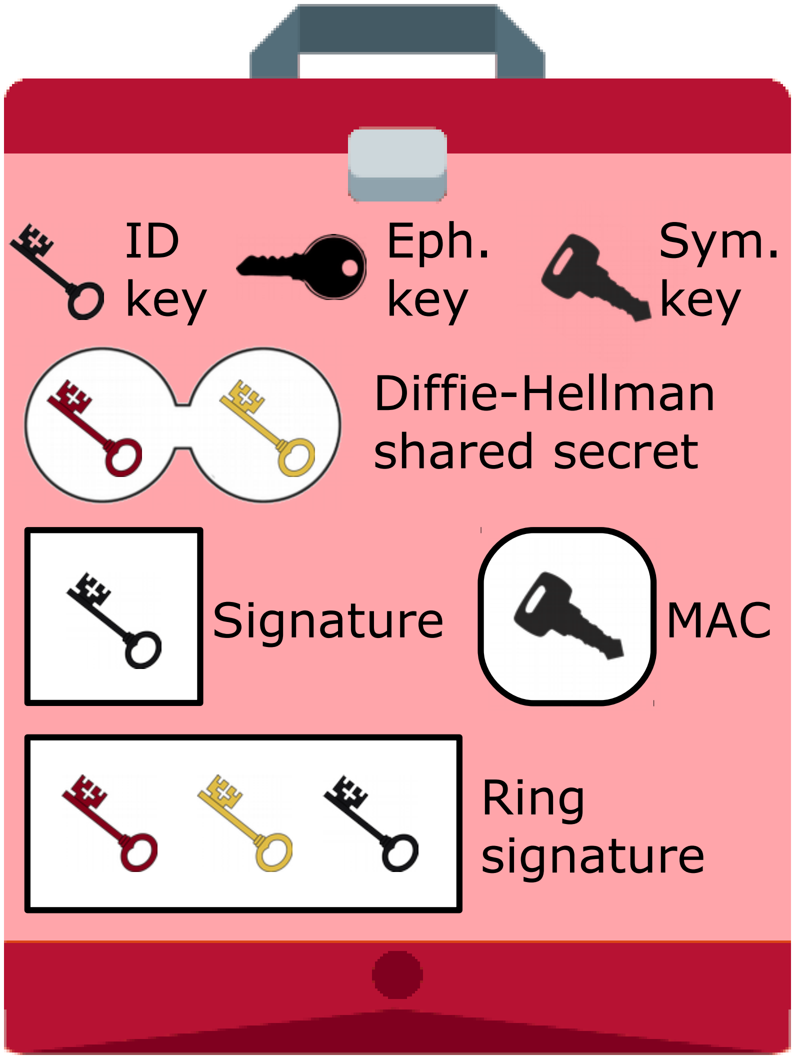


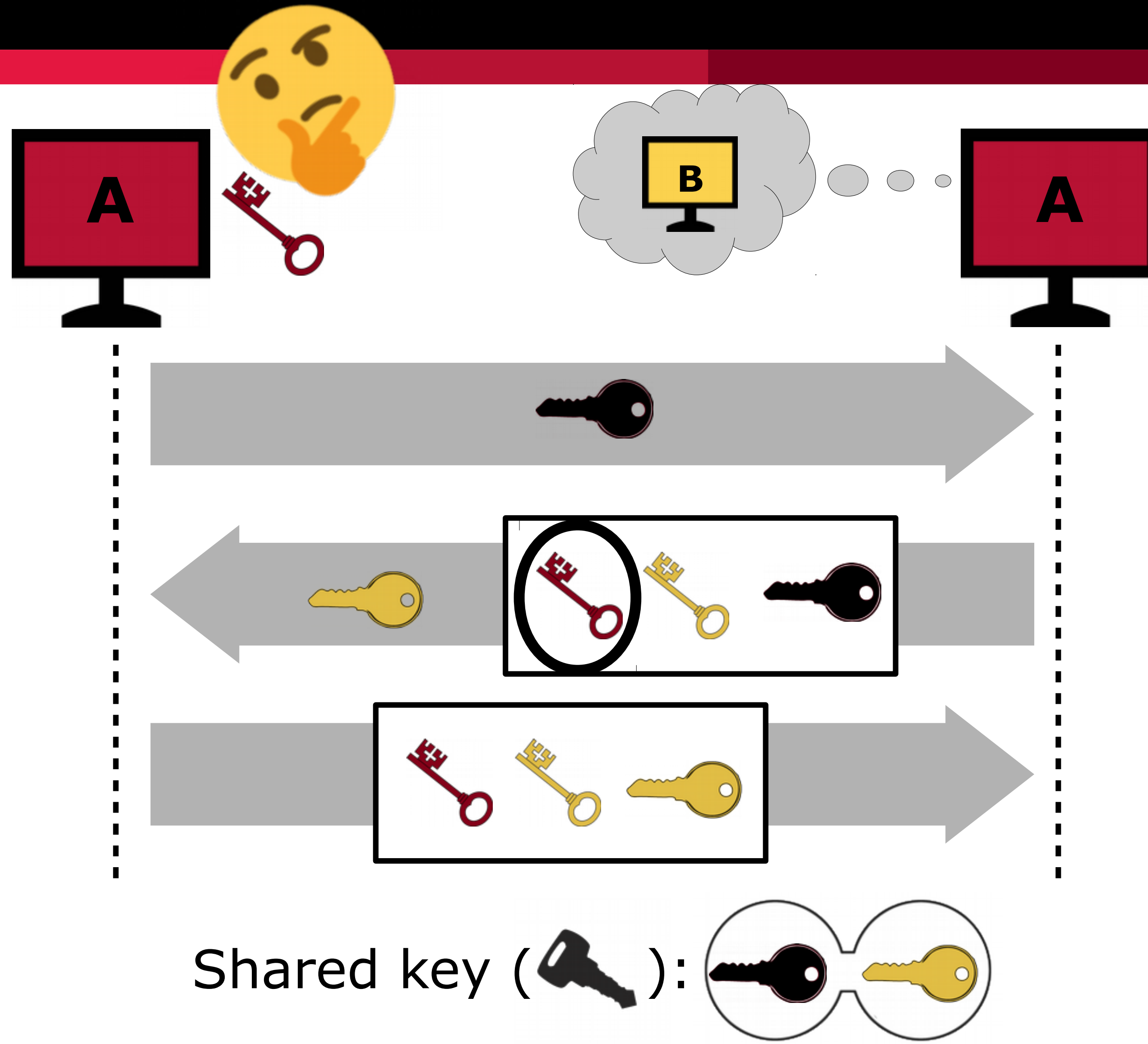
DAKEZ: Offline Deniability





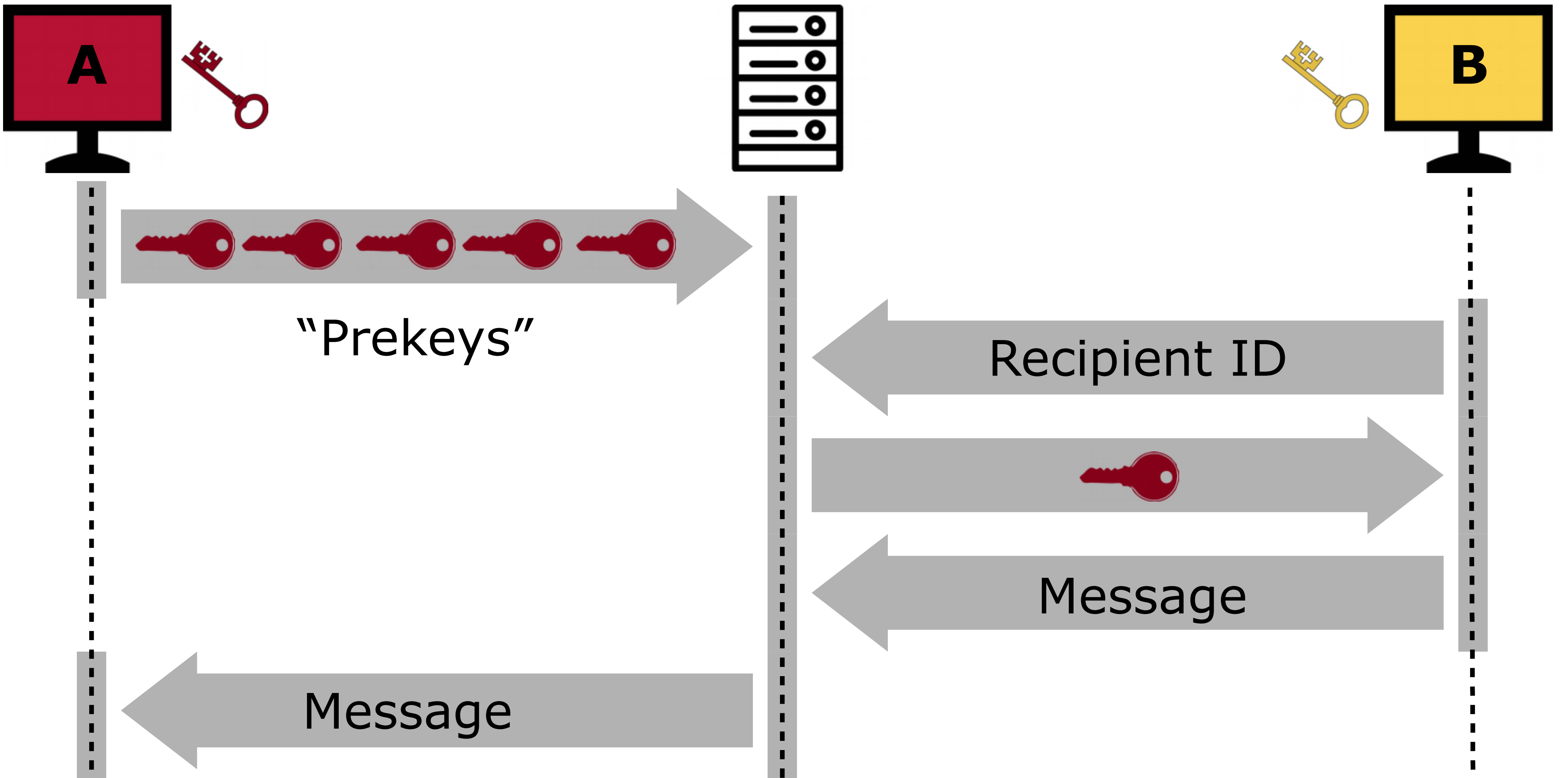
DAKEZ: Online Deniability



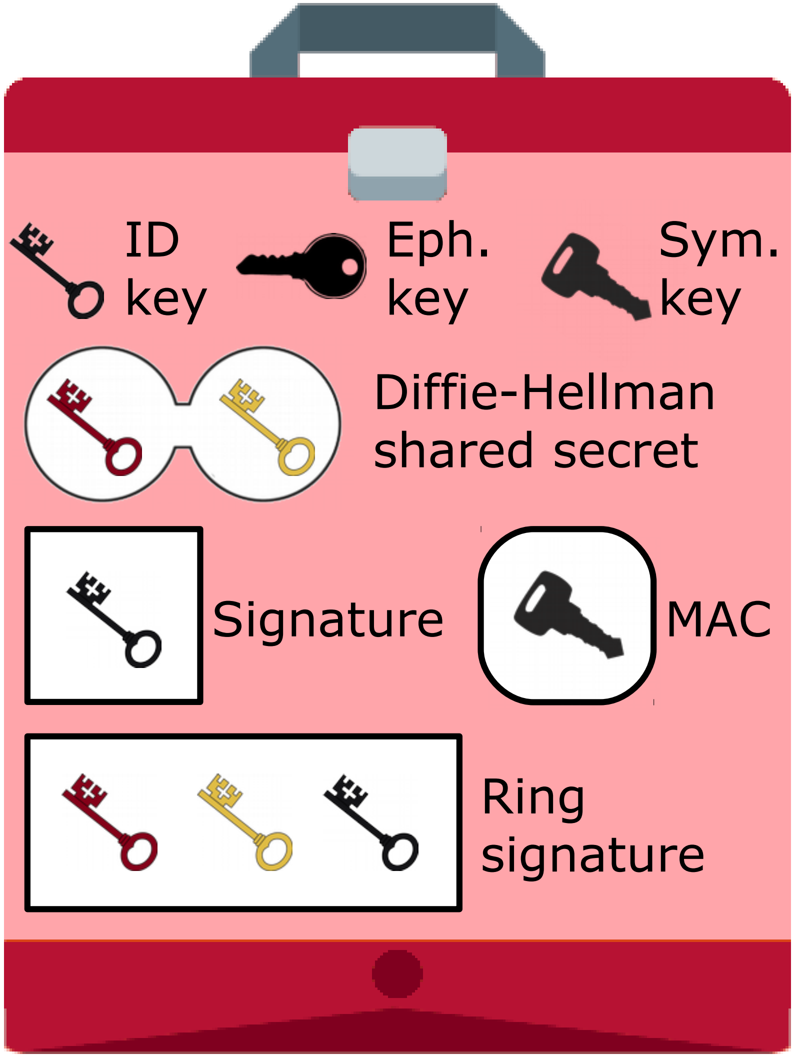


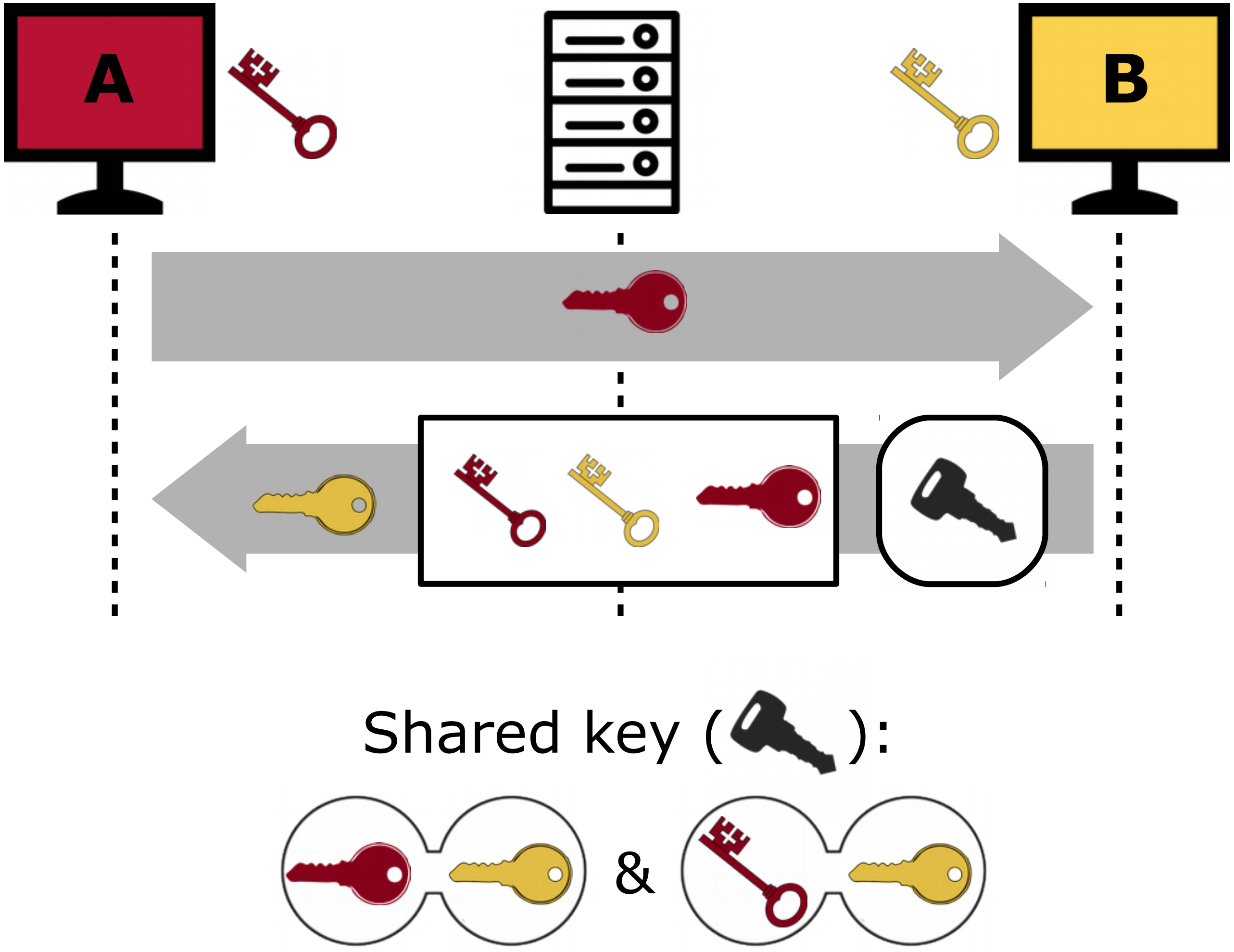
Mobile?

Mobile Use

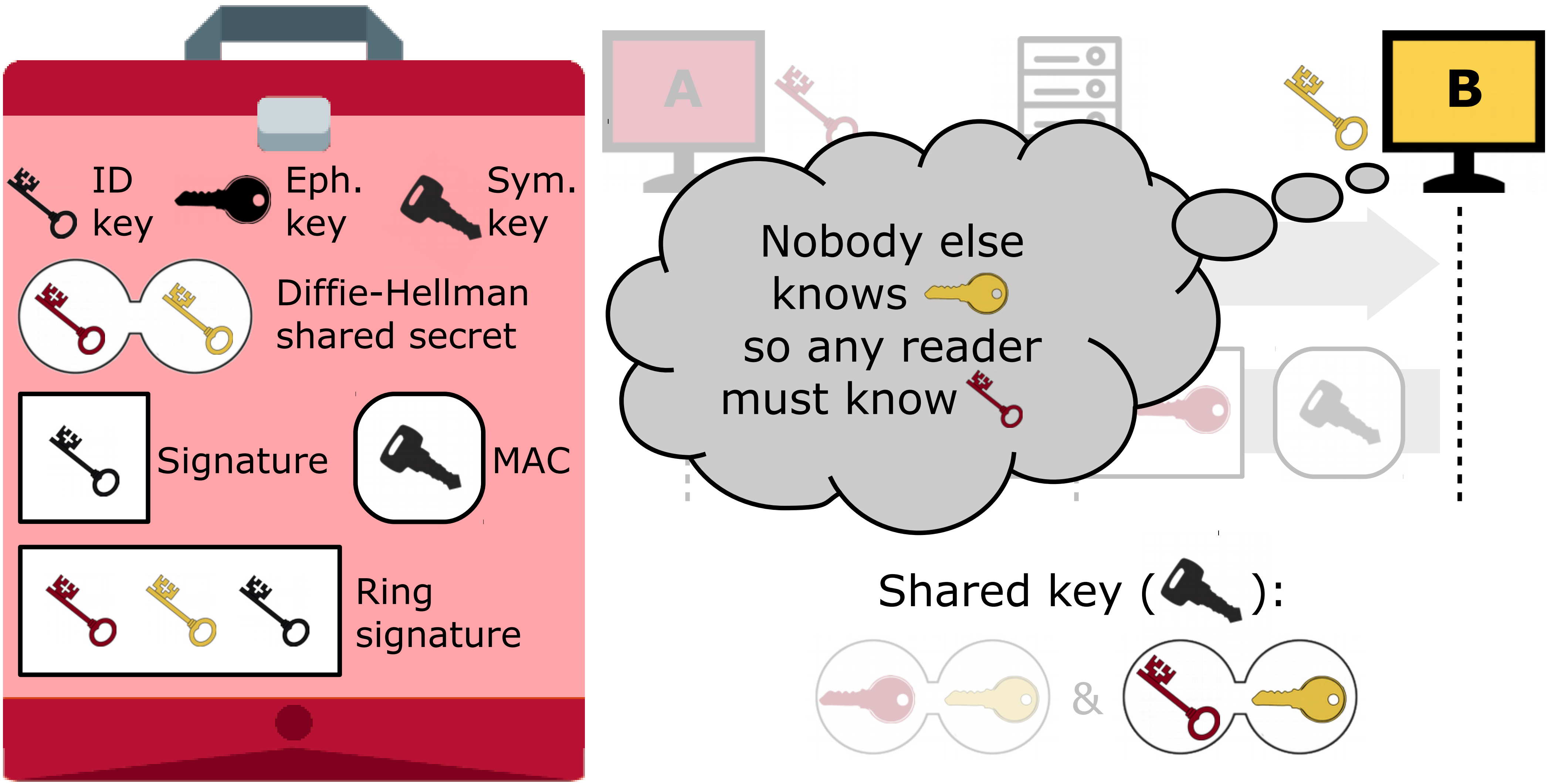


ZDH


ID
key
Eph.
key
Sym.
key
Diffie-Hellman
shared secret
Signature
MAC
Ring
signature

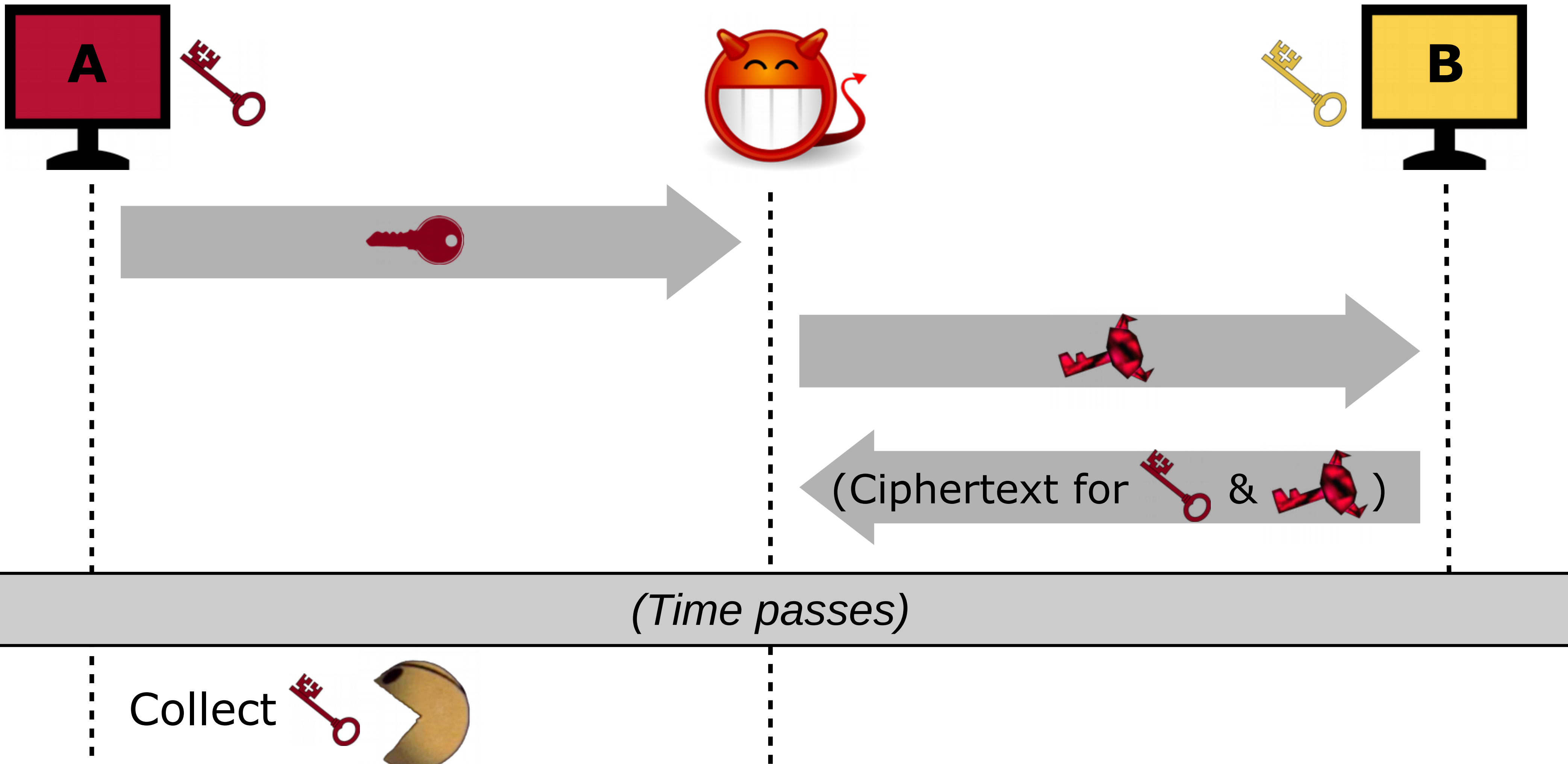

A
B
Shared key ( ):
&

ZDH: Authentication

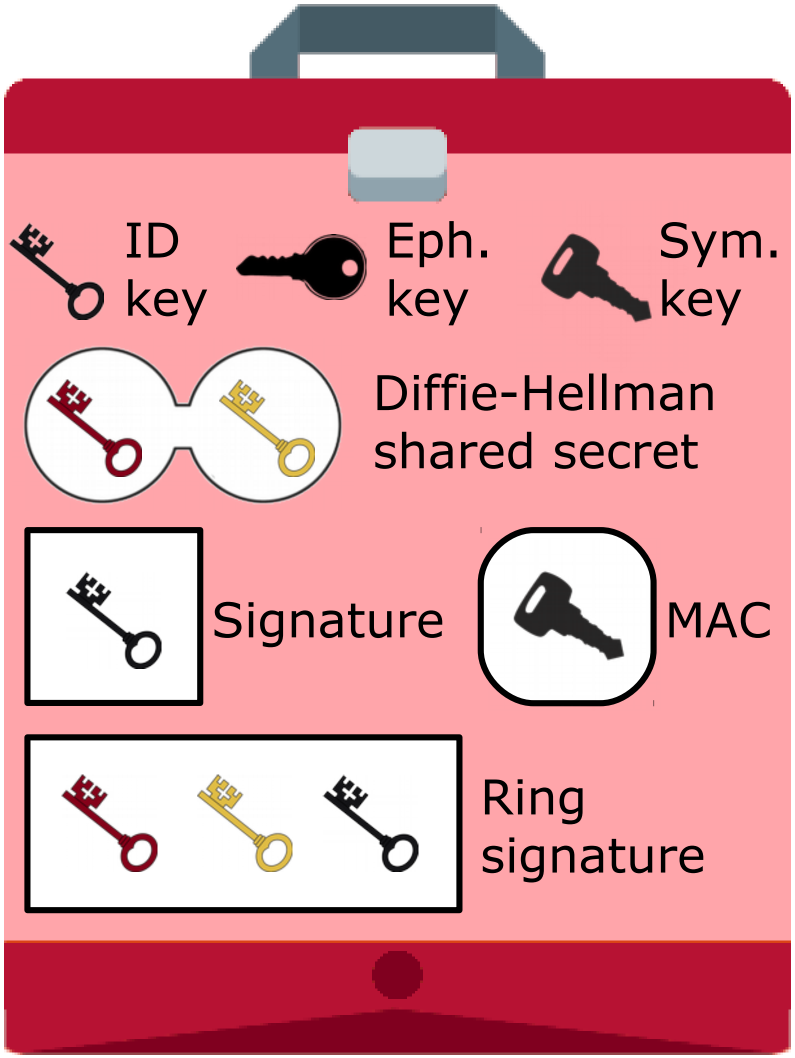


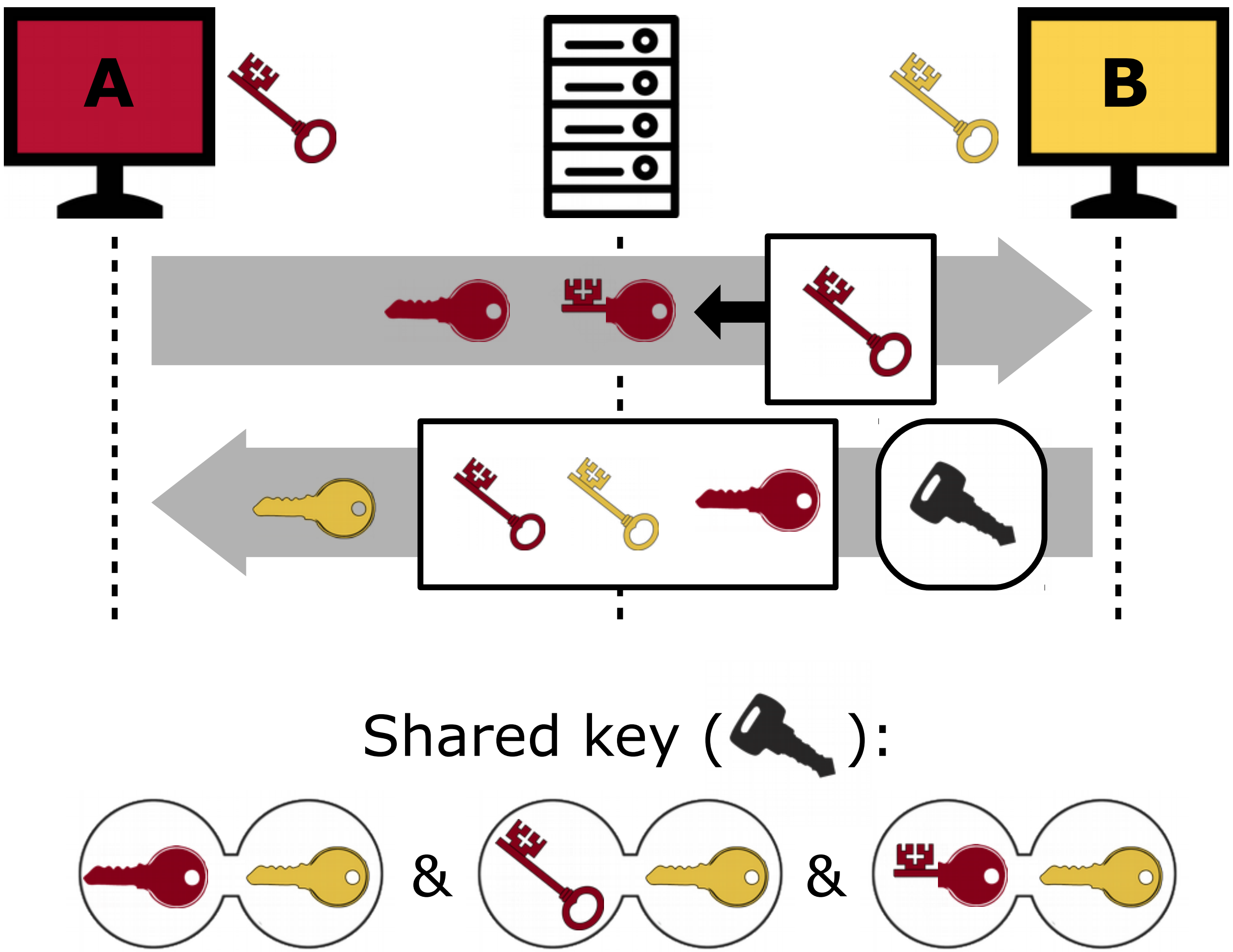
Weak Forward Secrecy

(Like Signal, originally)



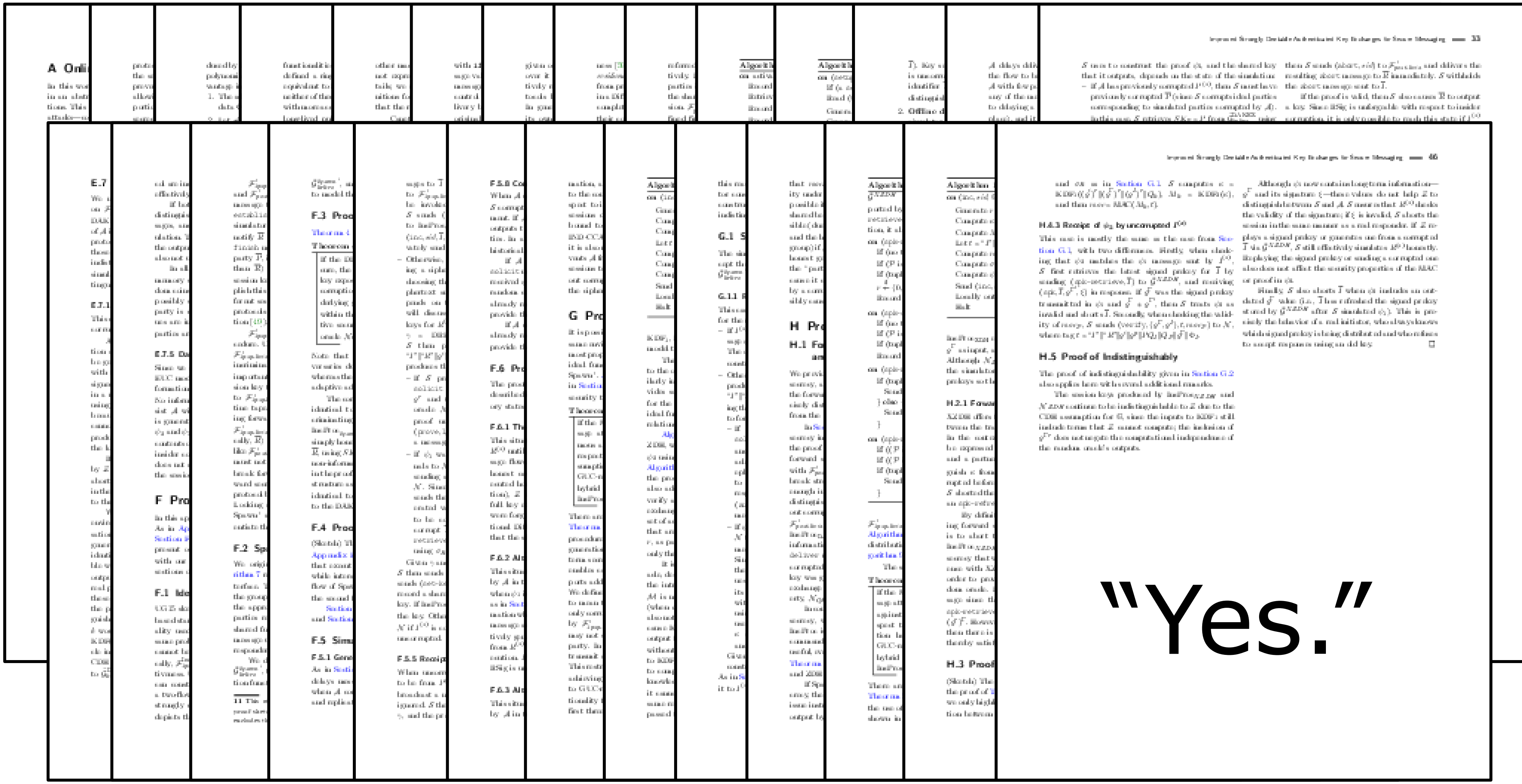
XZDH


ID key
Eph. key
Sym. key
Diffie-Hellman shared secret
Signature
MAC
Ring signature


A
B
Shared key ( ):
&
&

Is This Secure?

Is This Secure?



OTRv4 Adoption

- External adoption: OTRv4 team

No evidence of communication: Off-The-Record Protocol version 4

Ola Bini
Centro de Autonomia Digital
ola@autonomia.digital

Sofía Celi
Centro de Autonomia Digital
sofia@autonomia.digital

1. INTRODUCTION

Cryptography is commonly used to secure private communications over the Internet. One way is to try to protect casual personal conversations, in a way that mimics the idea of a

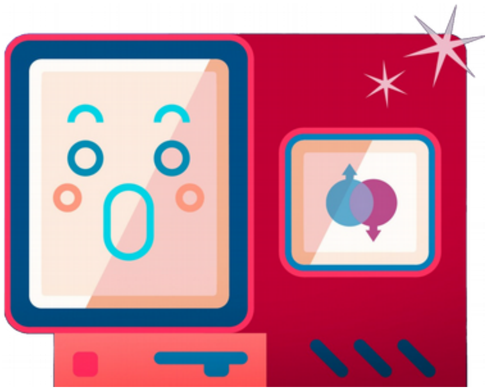
it, as no cryptographic evidence of it can exist. However, the current secure messaging tools only allow for limited deniability, where the privacy and security of the participants engaging in a conversation can be compromised. With this in mind, we designed

Performance

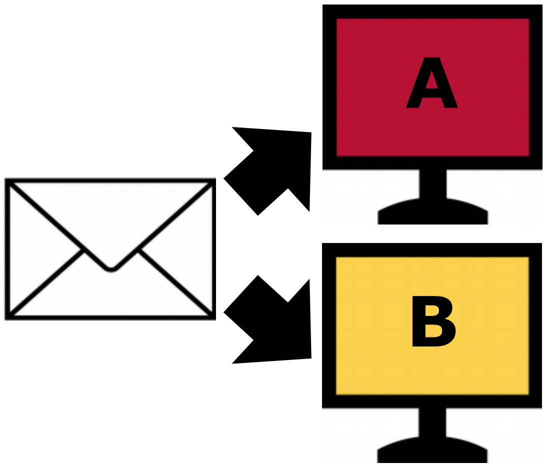
	SIGMA-R (OTRv3)	**DAKEZ (OTRv4)**	3DH	**ZDH**	X3DH (Signal)	**XZDH (OTRv4)**
Key Gen. (ms)	0.0240	0.0440	0.0228	0.0429	0.0240	0.0444
Key Exch. (ms)	0.3478	1.094	0.4229	0.778	0.5533	0.9217
ID Key (bytes)	32	32	32	32	32	32
Prekey (bytes)	-	-	32	32	32 & 96	32 & 96
Key Exch. (bytes)	272	464	80	304	80	304

Extras in the Paper

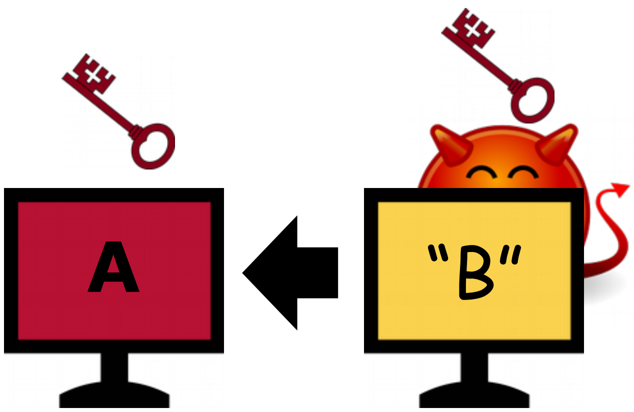
Extras in the Paper



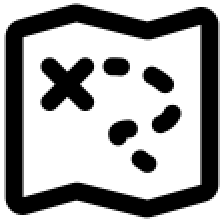
Quantum-resistant transitional security



Efficient dual-receiver encryption



Defeating key-compromise impersonation



Implementation details & advice

Summary

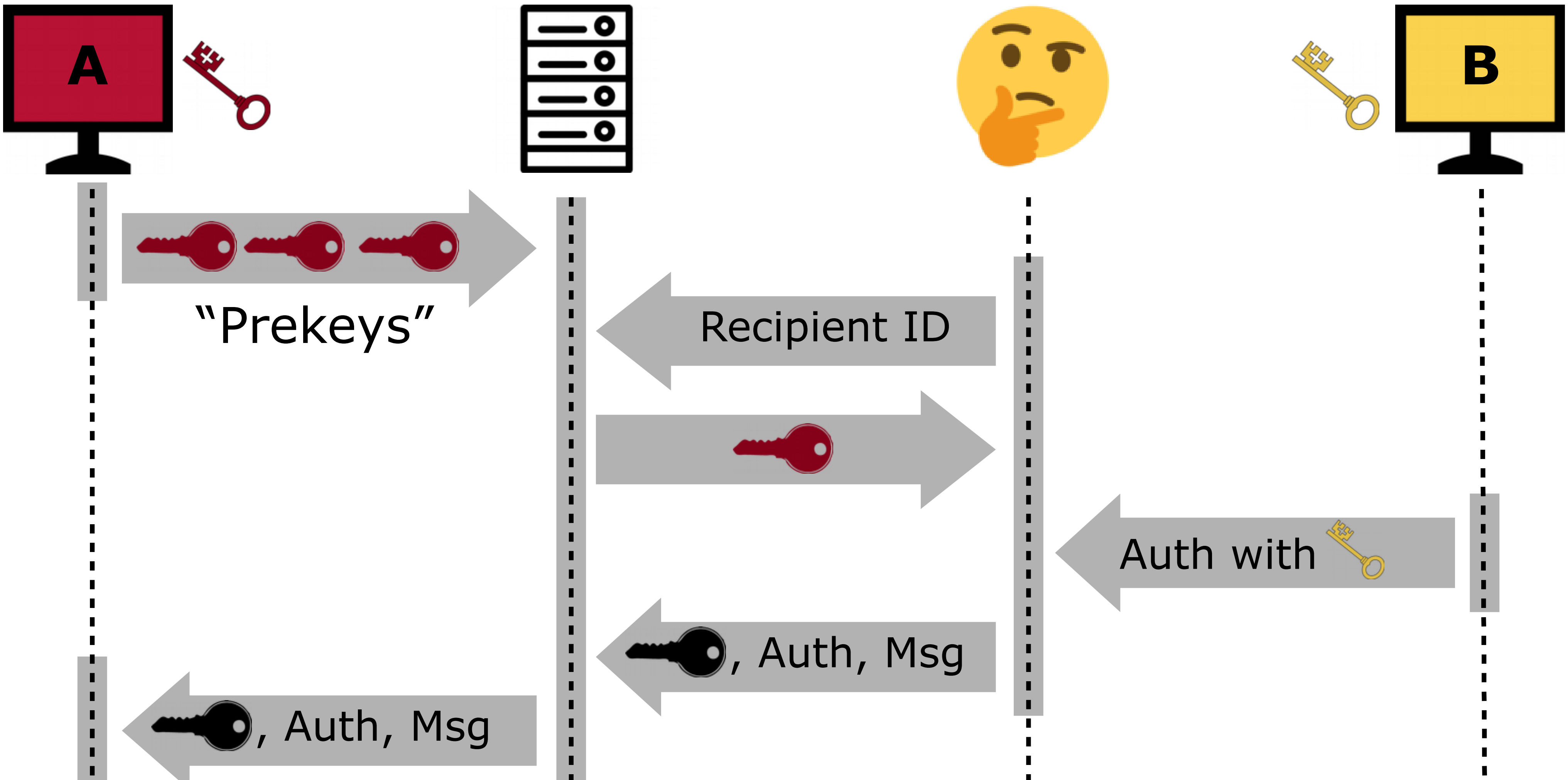
- New key exchanges: DAKEZ, (X)ZDH
- Secure connection, eponymous, no all-verifier authentication required? Use these!
- Code & data: crysp.org/software/dakez_xzdh
- Come see OTRv4 at HotPETs
- Coming soon: group messaging

Thank you!

njunger@uwaterloo.ca

You've Activated My Bonus Slides!!!

Limited Online Deniability



RSDAKE and Spawn

- Standard model → Random oracle model
  - Obscure assumptions → common assumptions
  - Seconds → milliseconds
  - Improved security (contributiveness, forward secrecy)
- RSDAKE → DAKEZ
- Spawn → ZDH

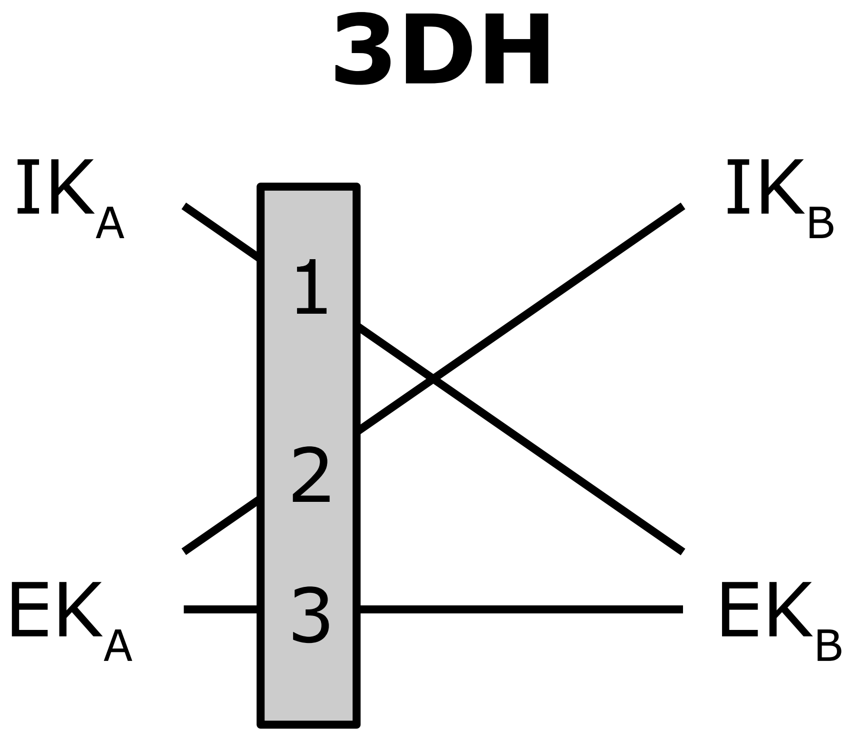
DAKE Comparison

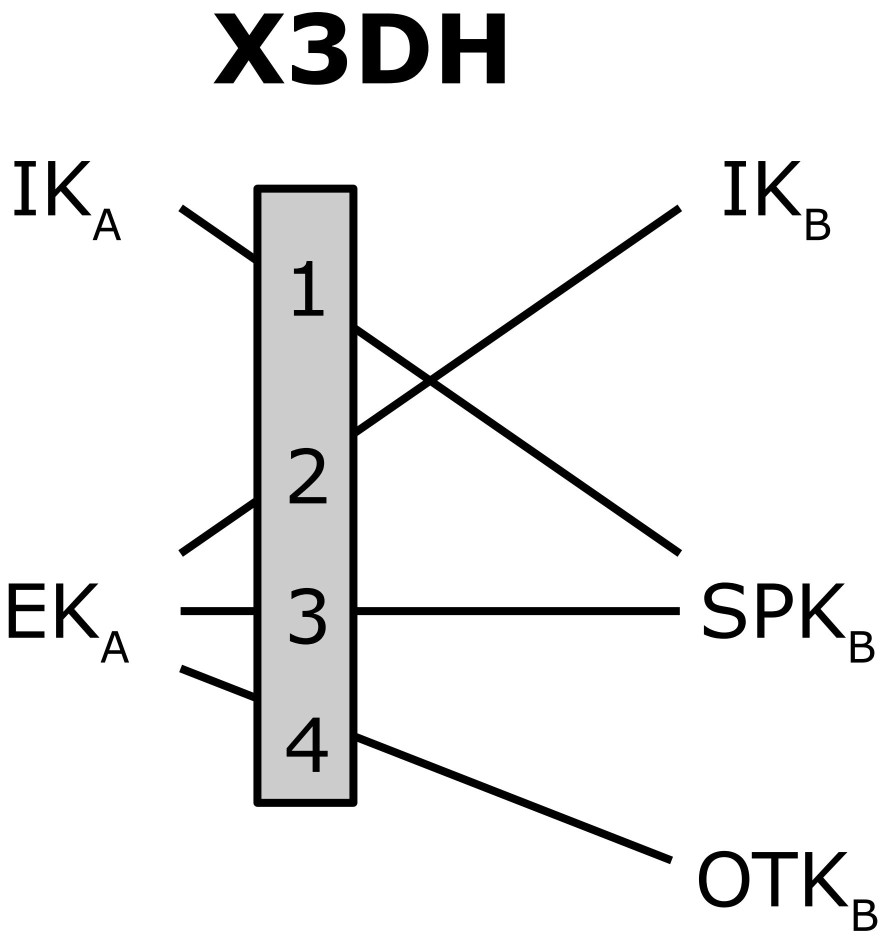
Table 1. Comparison of DAKE features, computational performance, and size requirements

	ECDH	3DH	X3DH	SIGMA-R	Φ_{idre}	RSDAKE	Spawn	DAKEZ	Spawn$^+$	ZDH	XZDH
Offline Deniable	●	●	○	○	●	●	●	●	●	●	●
Online Deniable	●	-	-	-	●	●	○	●	○	○	○
Authenticated	-	●	●	●	●	●	●	●	●	●	●
Non-Interactive	●	●	●	-	-	-	●	-	●	●	●
Forward Secrecy	-	-	○	●	●	●	-	●	-	-	○
Proof Model	SM	ROM	ROM	ROM	SM	SM	SM	ROM	ROM	ROM	ROM
Public Key Generation [ms]	-	0.0228 (0.0012)	0.0240 (0.0013)	0.0240 (0.0012)	0.40 (0.01)	206 (8)	206 (4)	0.0440 (0.0016)	0.0429 (0.0016)	0.0441 (0.0018)	0.0444 (0.0017)
Exchange [ms]	0.1733 (0.0033)	0.4229 (0.0050)	0.5533 (0.0056)	0.3478 (0.0048)	13 (2)	6 630 (50)	3 390 (20)	1.094 (0.014)	1.3683 (0.0082)	0.778 (0.013)	0.9217 (0.0069)
Flows	2	2	2	4	9	3	2	3	2	2	2
Public Key [B]	-	32	32	32	415	395	992	32	32	32	32
Prekey [B]	-	32	32+96	-	-	-	938	-	32	32	32+96
Exchange [B]	64	80	80	272	5 140	7 598	73 763	464	512	304	304

● = provides property; ○ = partially provides property; - = does not provide property / not applicable; SM = standard model; ROM = random oracle model. Standard deviations are in parentheses. "Forward secrecy" is the strong variant [14] (all schemes have weak forward secrecy). Prekeys are listed as (one-time)+(signed) sizes.

Signal Deniability

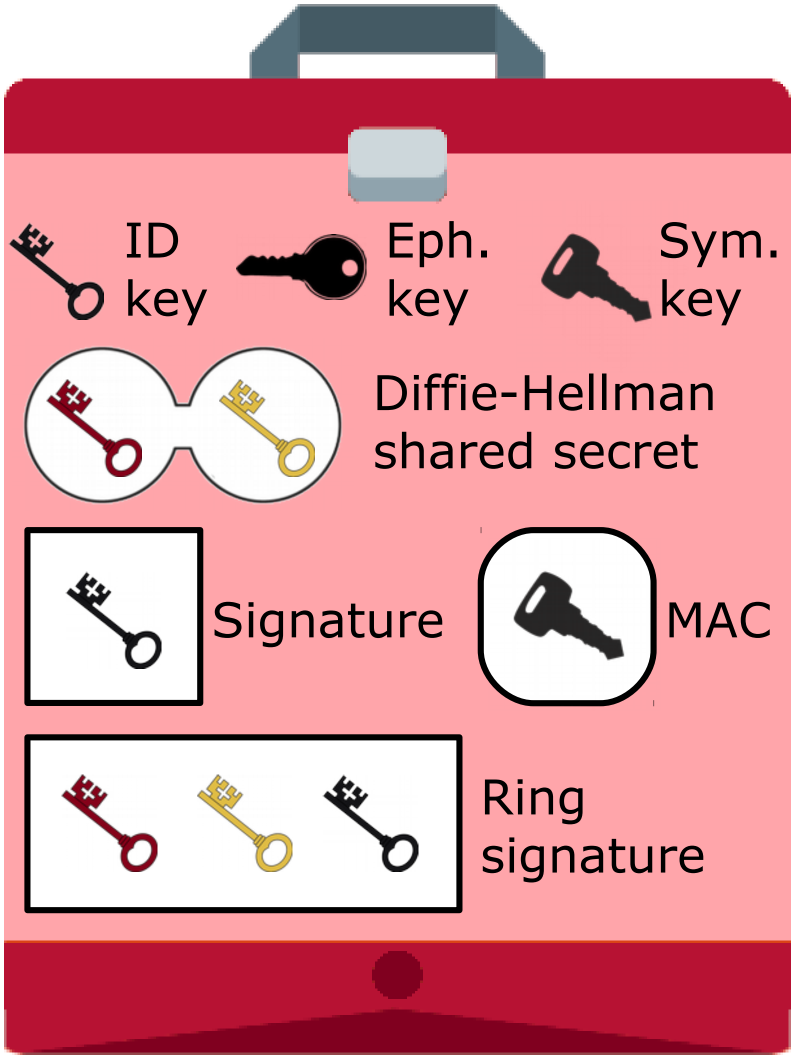


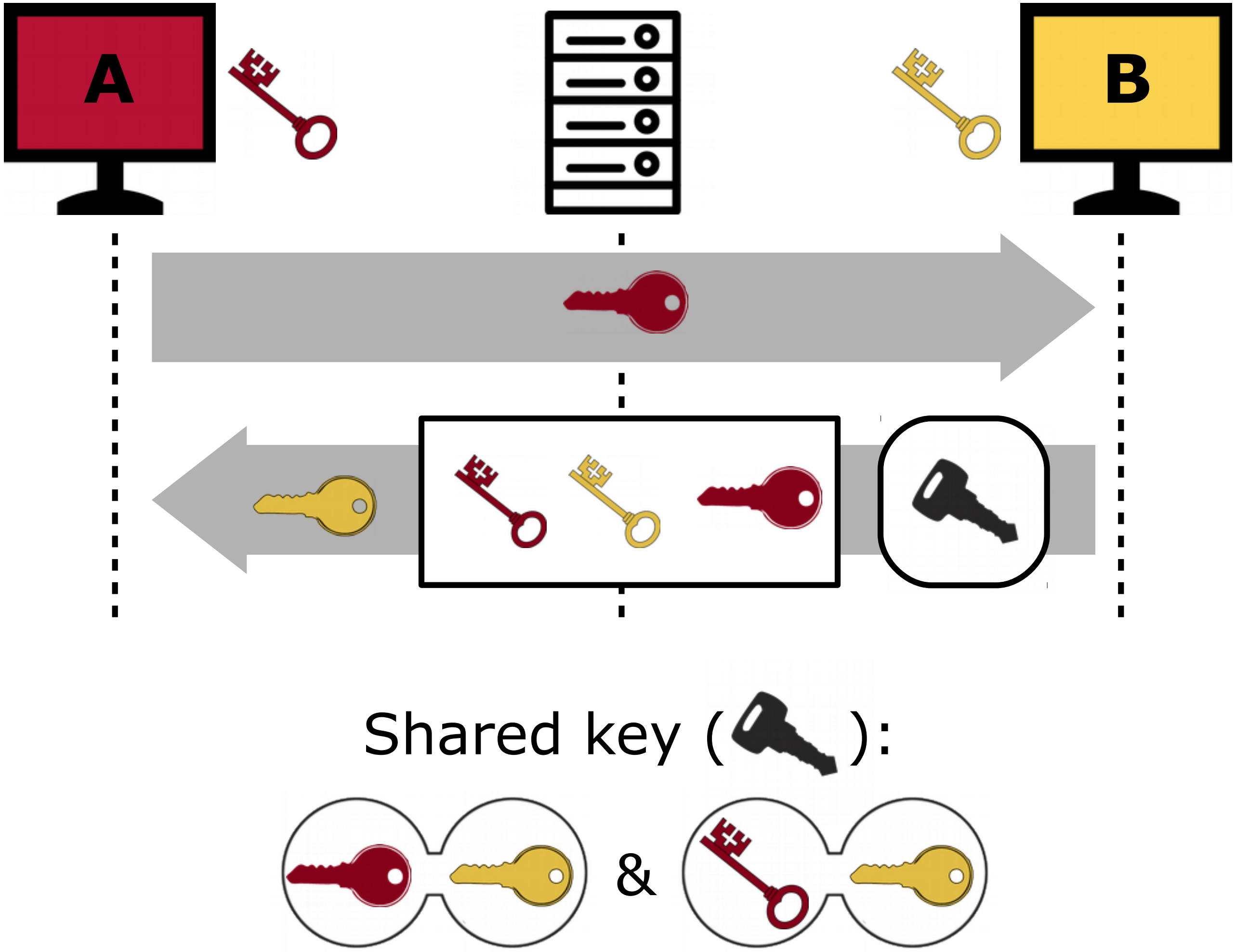


Lack of Contributiveness

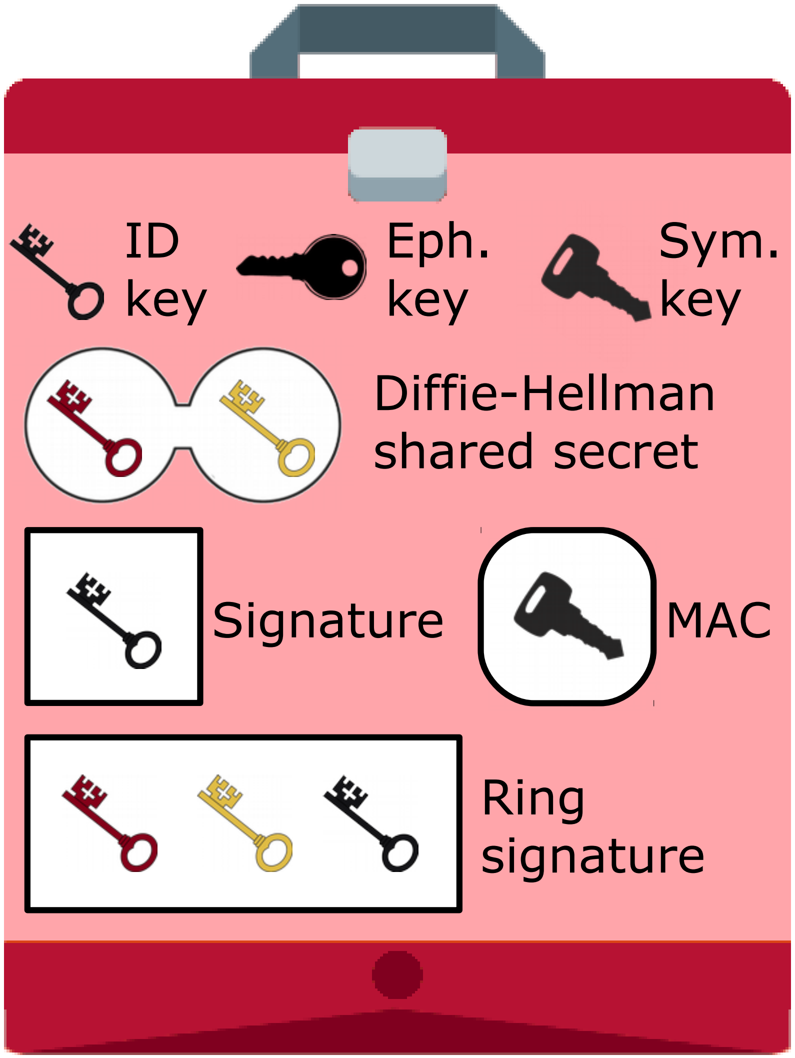
- **Problems** with non-contributory:
  - Can coerce a client to use a known secret
  - Can use a secret known to a third-party, allowing them to decrypt without their consent
- **Non-problems** with non-contributory:
  - Contributiveness does not prevent desirable bits
  - Contributiveness does not defend against weak PRNGs

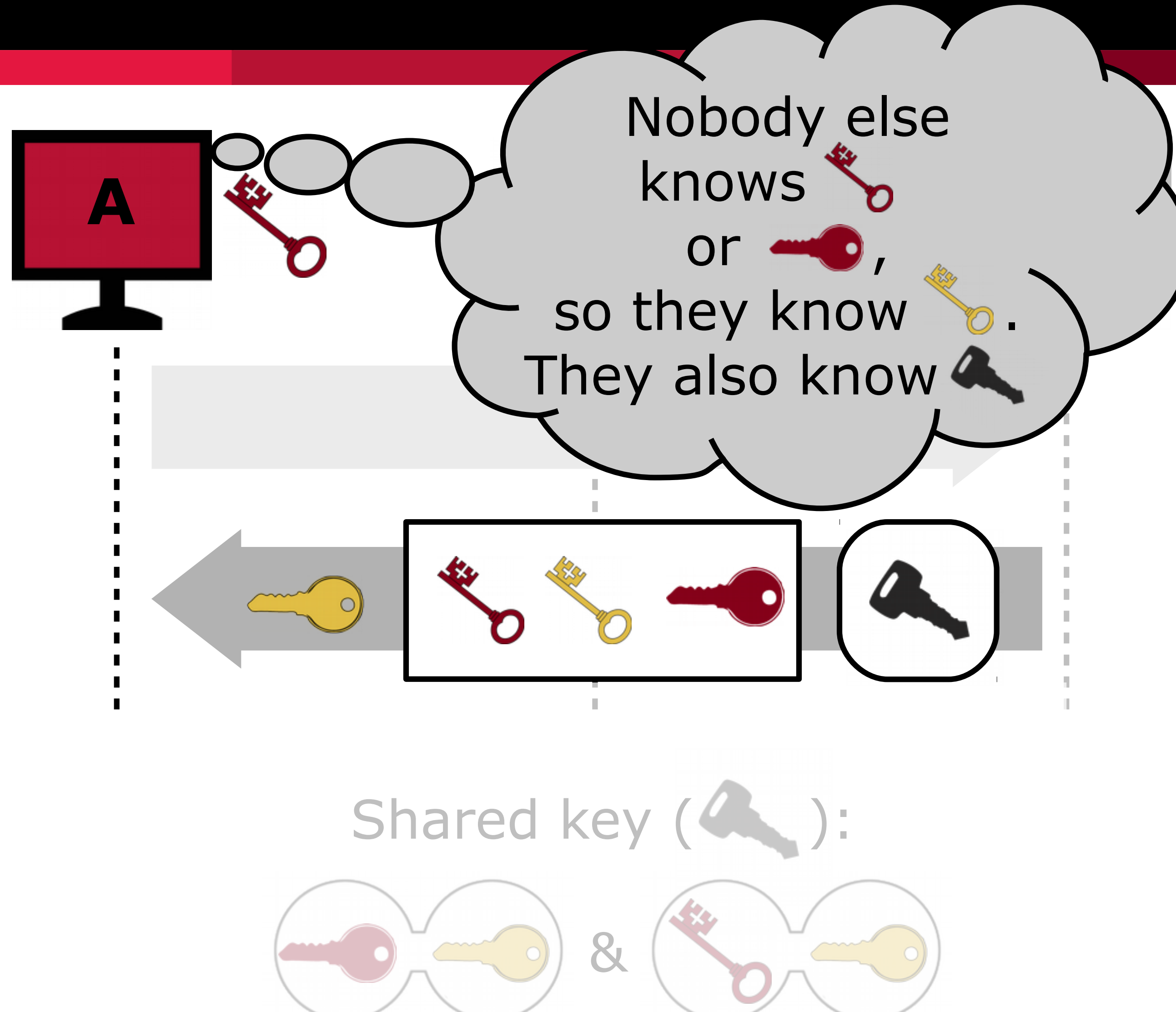
ZDH


ID key
Eph. key
Sym. key
Diffie-Hellman shared secret
Signature
MAC
Ring signature

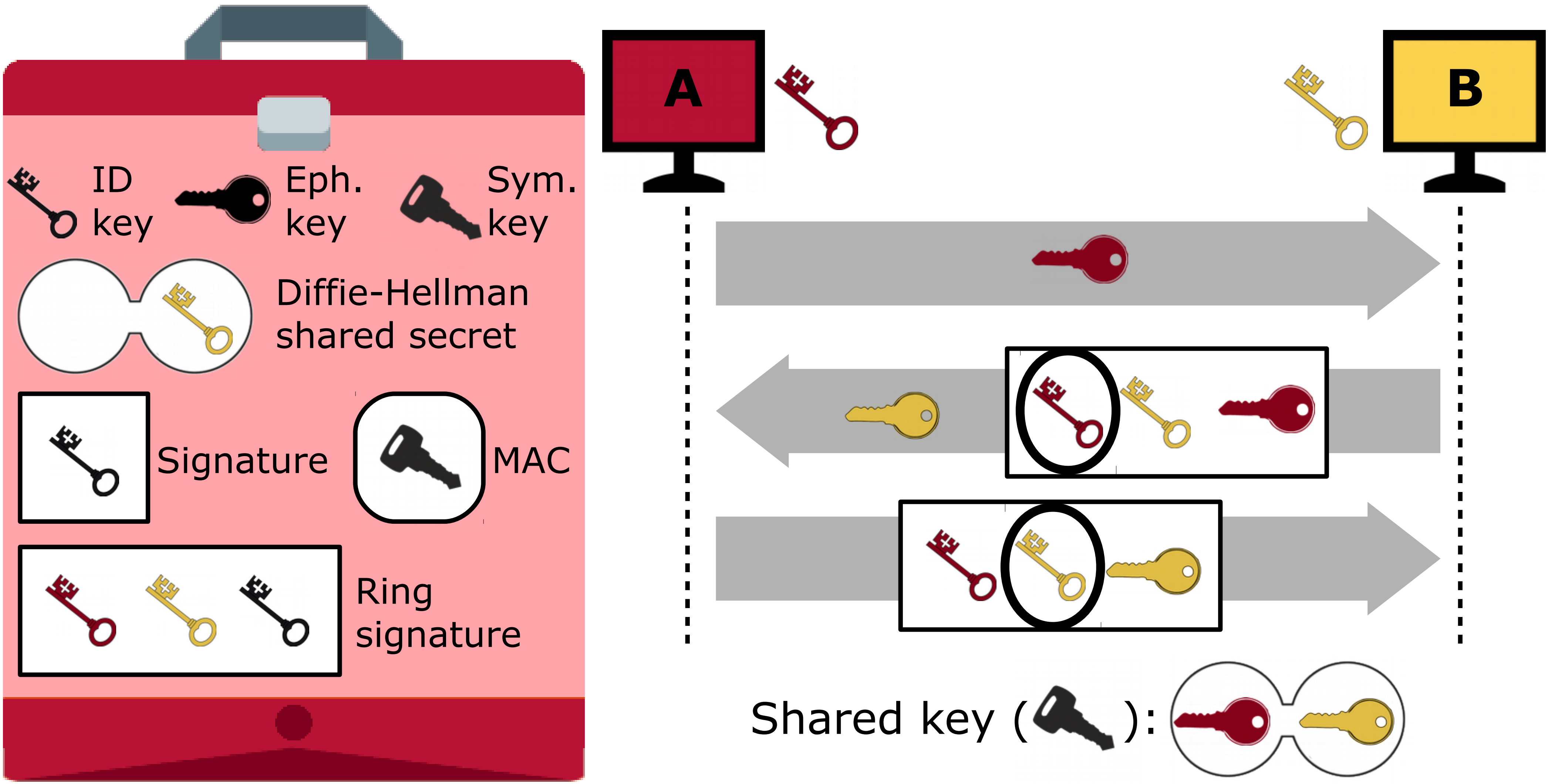

A
B
Shared key ( ):
&

ZDH: Authentication





Mitigating KCI Attacks



Online Deniability Attack for Signal

- (Alice is coerced by Judson)
- Alice downloads Bob's prekey: IK_B, SPK_B, $Sig(IK_B, Encode(SPK_B))$
- Judson generates key pair with public EK_A
- Alice provably reveals $DH(IK_A, SPK_A)$
- Alice sends EK_A to Bob
- Judson can compute the secret, Alice cannot

Quantum Transitional Security

- Authenticate quantum KEM, like CECPK1

Scheme	Δ Time [ms]	PQ_I [bytes]	Q_R [bytes]
New Hope	+0.0542 (0.0041)	+1824	+2048
SIDH	+63.8 (1.5)	+768	+768

DAKEZ

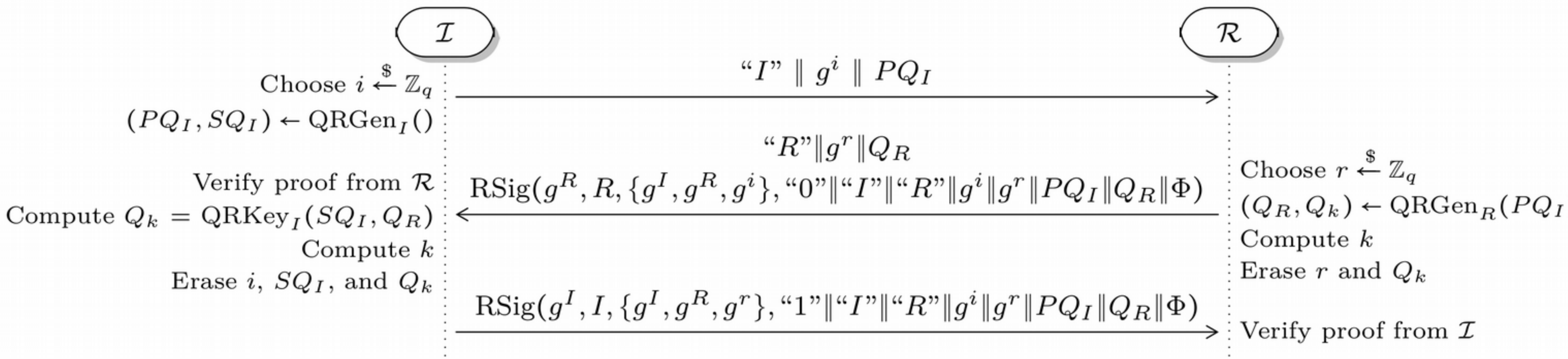


Fig. 2. The DAKEZ protocol. Φ is shared session state. The shared secret is $k = \text{KDF}(g^{ir} \parallel Q_k)$.

ZDH & XZDH

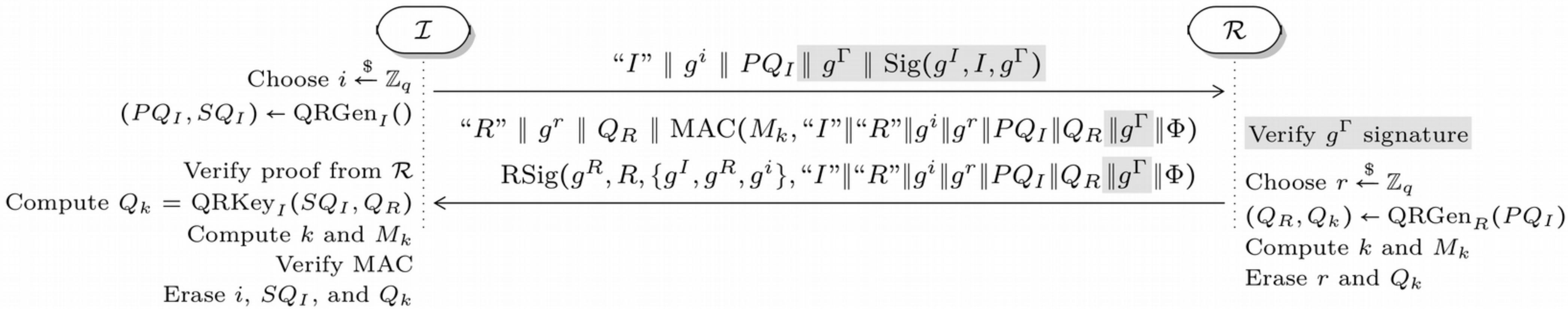


Fig. 4. A ZDH/XZDH exchange. Φ is shared session state. $\kappa = \mathsf{KDF}_1(g^{ir}\|g^{\Gamma r}\|g^{Ir}\|Q_k)$, $M_k = \mathsf{KDF}_2(\kappa)$ and the shared secret is $k = \mathsf{KDF}_3(\kappa)$. Shaded terms are used in XZDH only, and omitted for ZDH. In XZDH, g^Γ is a reusable signed prekey.