IMPROVED STRONGLY DENIABLE AUTHENTICATED KEY EXCHANGES FOR SECURE MESSAGING

Nik Unger

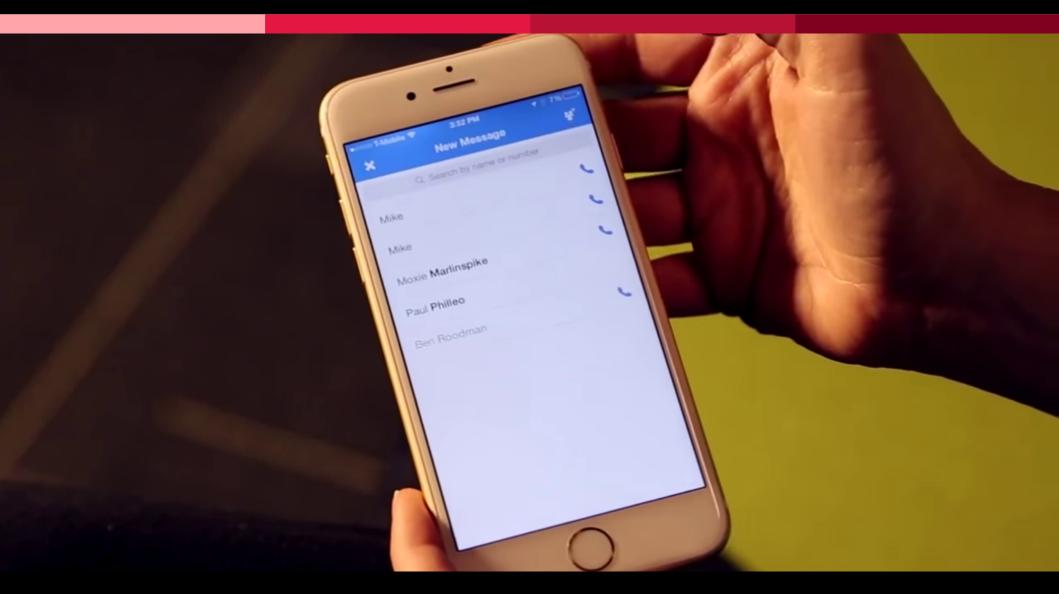
^{and} Ian Goldberg



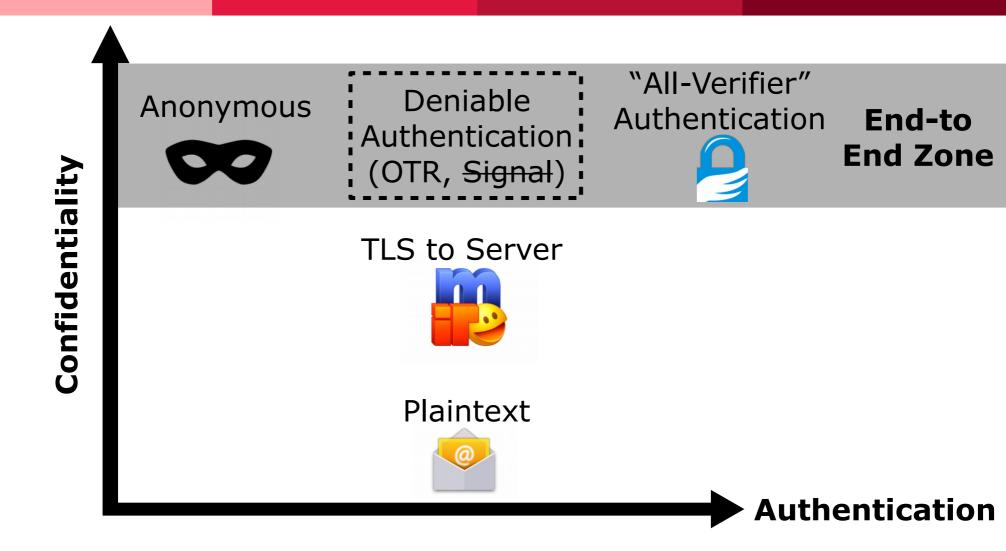
UNIVERSITY OF WATERLOO FACULTY OF MATHEMATICS David R. Cheriton School of Computer Science



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.

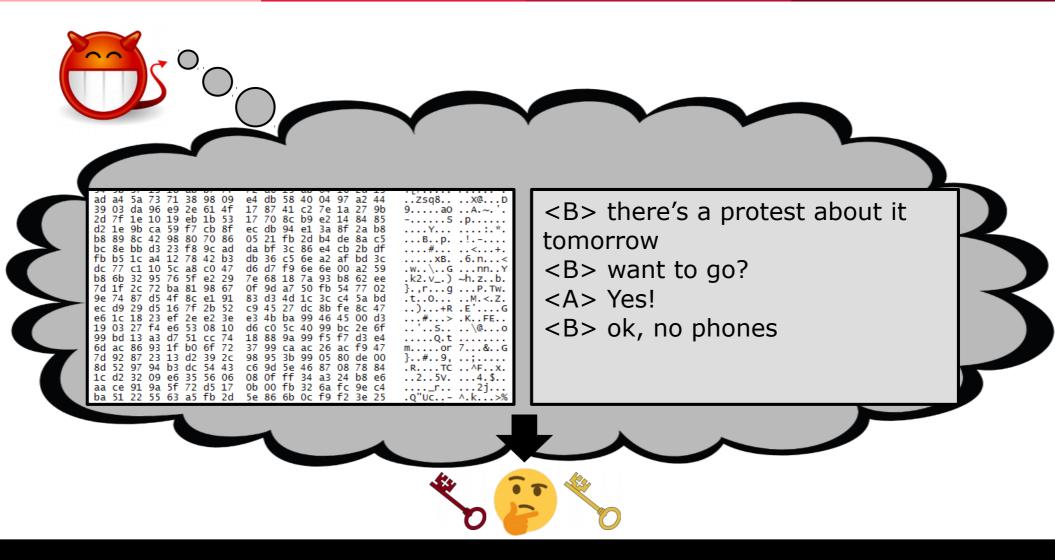
HillaryClinton.com uses Gmail to handle its mail and uses DKIM. Staffer Jennifer Palmieri, using her HillaryClinton.com email, replied to a Brazile email warning that Brazile was "worried" about Clinton's ability to answer a question about the

Deniable Messaging

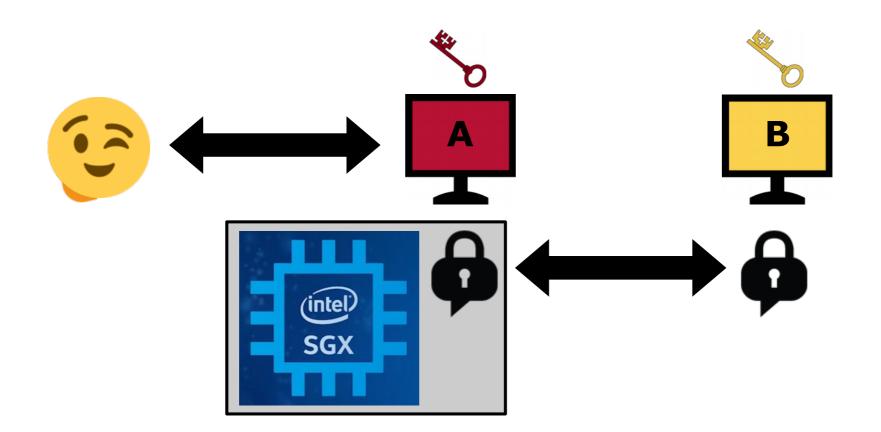
	Cryp Mag	
ad ad 5a 73 71 38 98 09 e4 db 58 40 04 97 a2 44 39 03 da 96 e9 2e 61 4f 17 87 41 c2 7e 1a 27 9b 2d 7f 1e 10 19 eb 1b 53 17 70 8c b9 e2 14 84 85 d2 1e 9b ca 59 f7 cb 8f ec db 94 e1 3a 8f 2a b8 b8 89 8c 42 98 80 70 86 05 21 fb 2d b4 de 8a c5 bc 8e bb d3 23 f8 9c ad da bf 3c 86 e4 cb 2b df fb b5 1c a4 12 78 42 b3 db 36 c5 6e a2 af bd 3c dc 77 c1 10 5c a8 c0 47 d6 d7 f9 6e 6e 00 a2 59 b8 6b 32 95 76 5f e2 29 7e 68 18 7a 93 b8 62 ee 7d 1f 2c 72 ba 81 98 67 0f 9d a7 50 fb 54 77 02 9e 74 87 d5 4f 8c e1 91 83 d3 4d 1c 3c c4 5a bd ec d9 29 d5 16 7f 2b 52 c9 45 27 dc 8b fe 8c 47 e6 1c 18 23 ef 2e e2 3e e3 4b ba 99 f5 f7 d3 e4 6d ac 86 93 1f b0 6f 72 37 99 ca ac 26 ac f9 47 7d 92 87 23 13 d2 39 2c 98 95 3b 99 05 80 de 00 8d 52 97 94 b3 dc 54 43 c6 9d 5e 46 87 08 78 84 1c d2 32 09 e6 35 56 06 08 0f ff 34 a3 24 b8 e6 aa ce 91 9a 5f 72 d5 17 0b 00 fb 32 6a fc 9e c4 ba 51 22 55 63 a5 fb 2d 5e 86 6b 0c f9 f2 3e 25		 there's a protest about it tomorrow want to go? <a> Yes! ok, no phones



Deniable Messaging



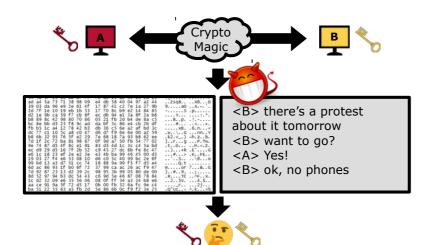
Deniable Messaging...?

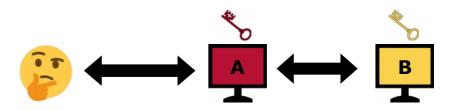


Offline vs. Online Deniability

Offline Deniability

Online Deniability





Deniable Messaging...?

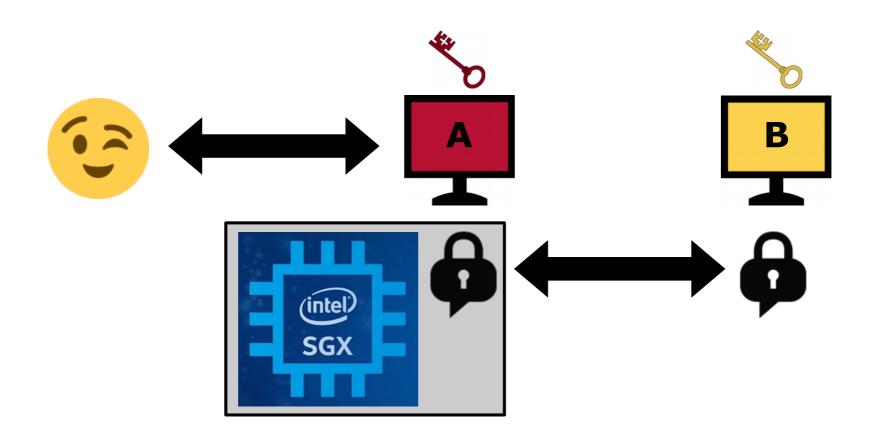
- See Appendix A
 - Attacks on OTRv3 and Signal
- Also see ia.cr/2018/424:

On The Use of Remote Attestation to Break and Repair Deniability

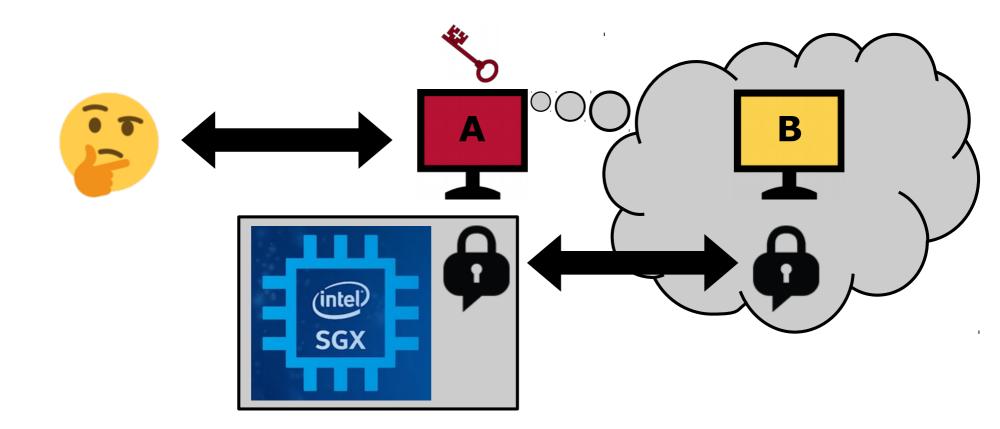
Lachlan J. Gunn Aalto University lachlan.gunn@aalto.fi

Ricardo Vieitez Parra Aalto University ricardo.vieitezparra@aalto.fi N. Asokan Aalto University asokan@acm.org

Deniable Messaging

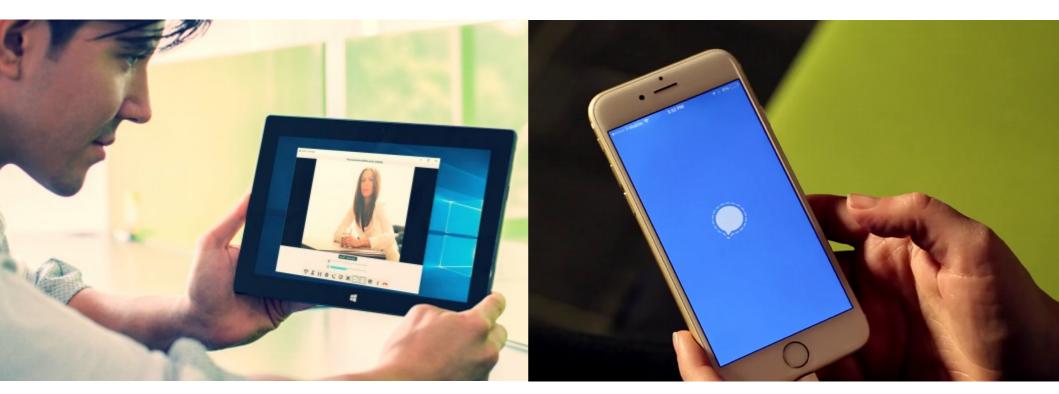


Deniable Messaging



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



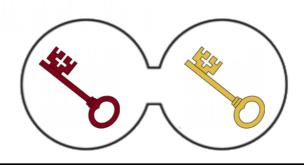
Identity key (long-term asymmetric)



Ephemeral key (short-term asymmetric)

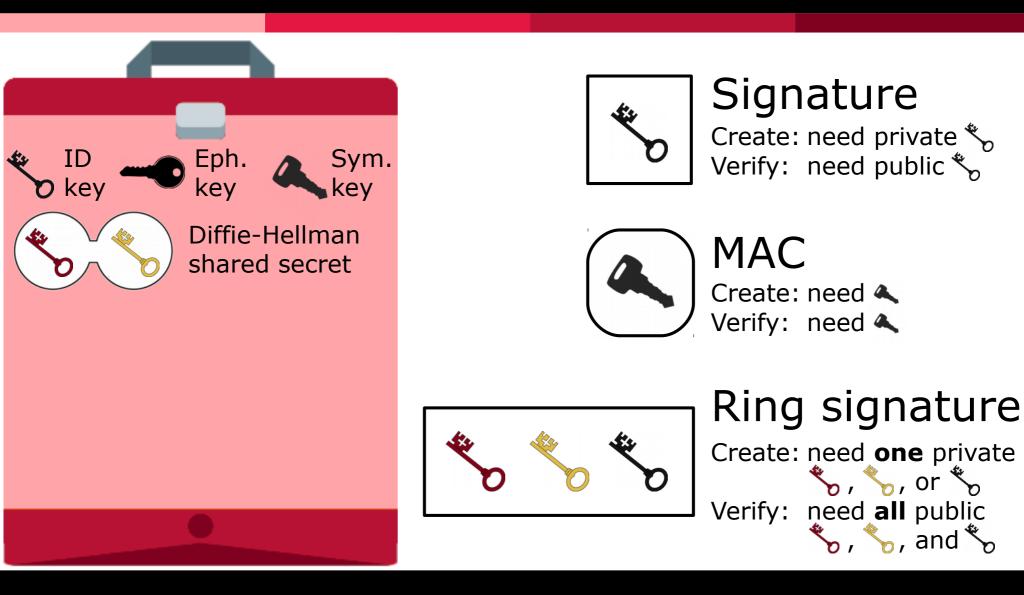


Shared session key (symmetric)

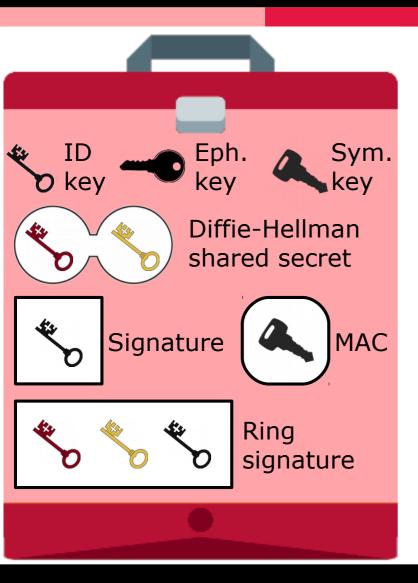


Diffie-Hellman shared secret

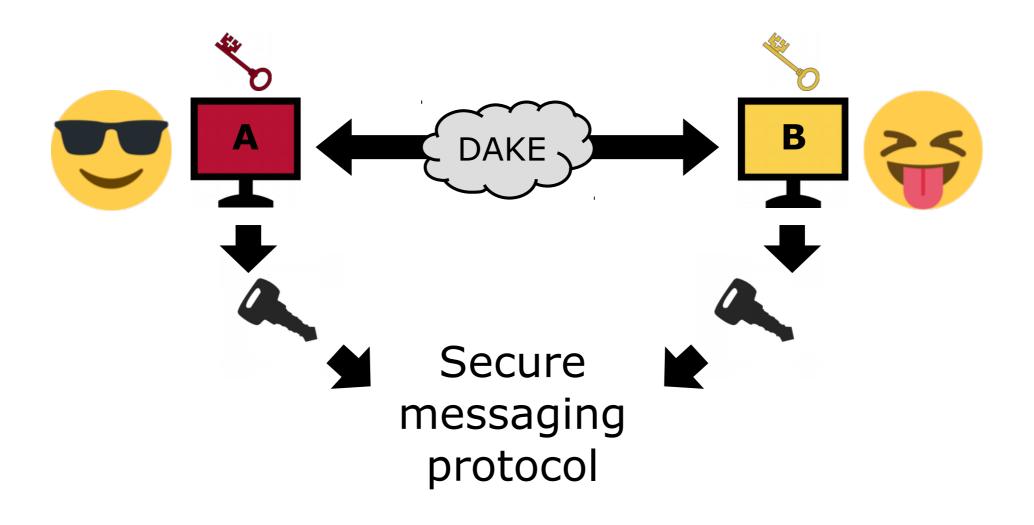
Crypto Toolbox



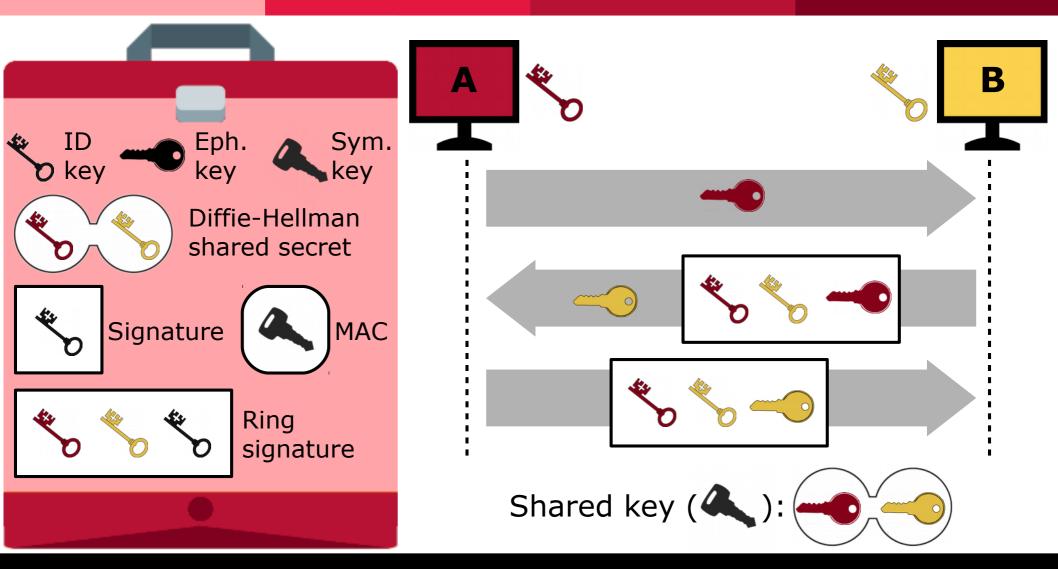
Crypto Toolbox



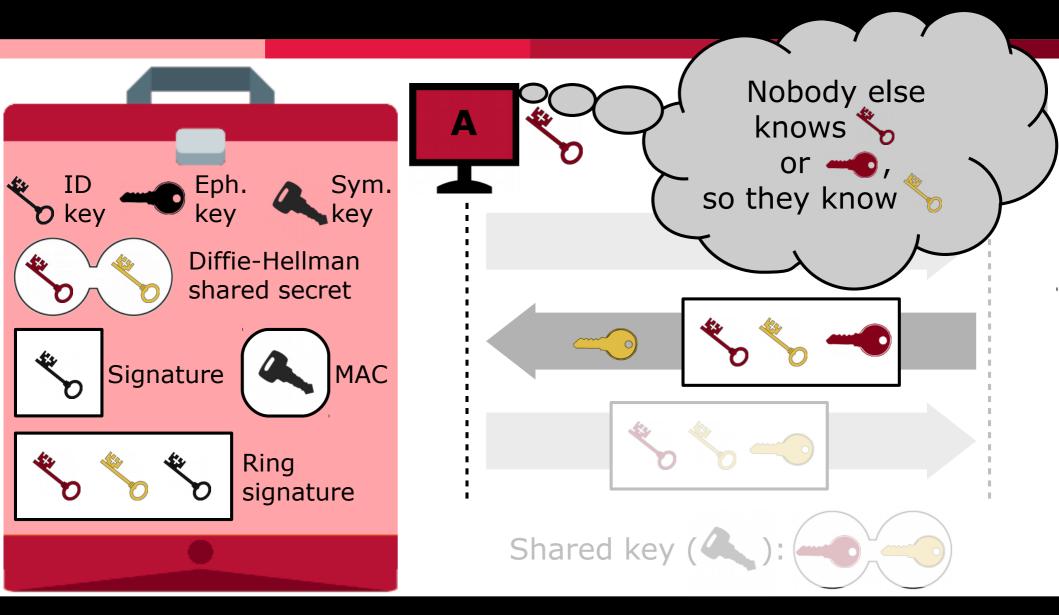
Deniable Authenticated Key Exchanges



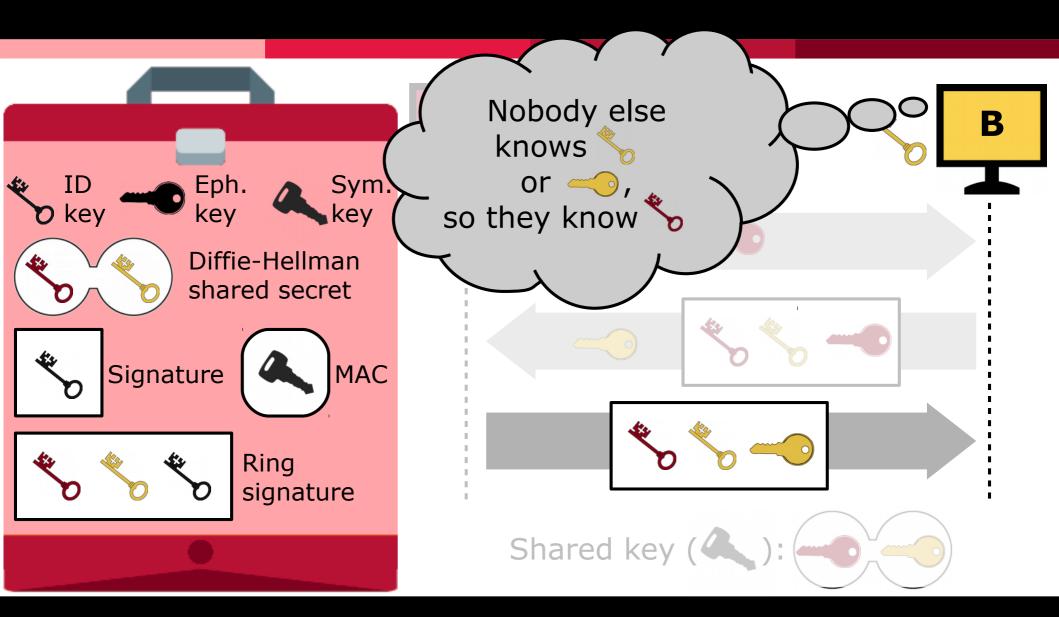




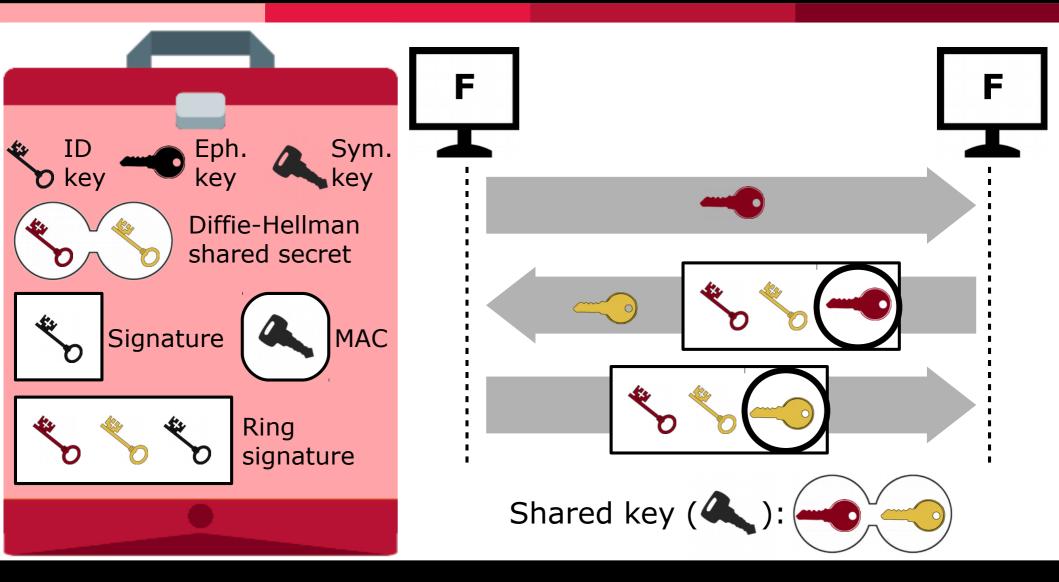
DAKEZ: Authentication



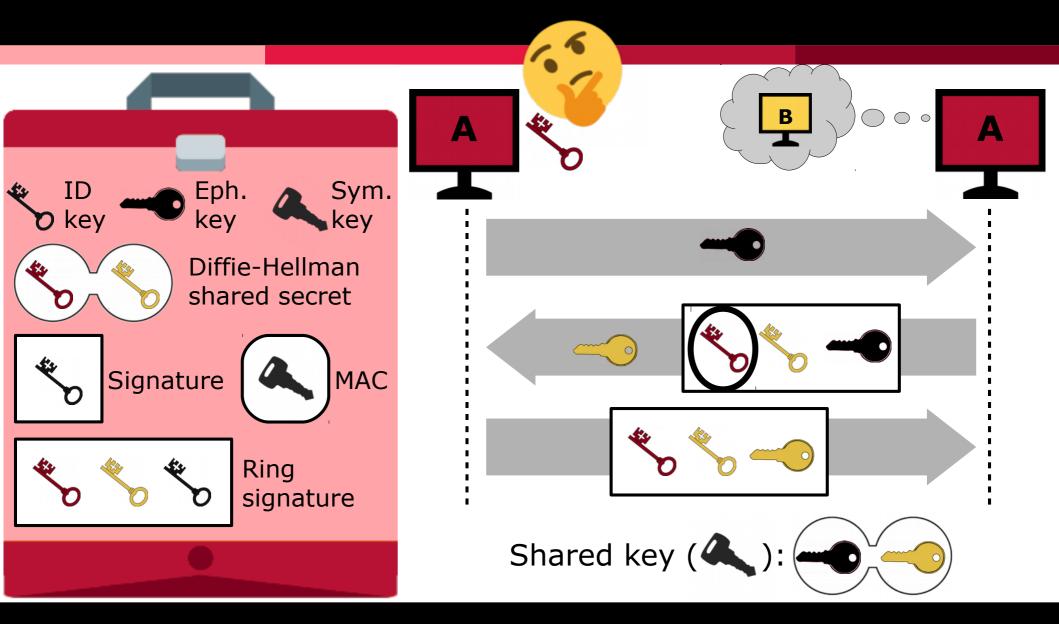
DAKEZ: Authentication



DAKEZ: Offline Deniability



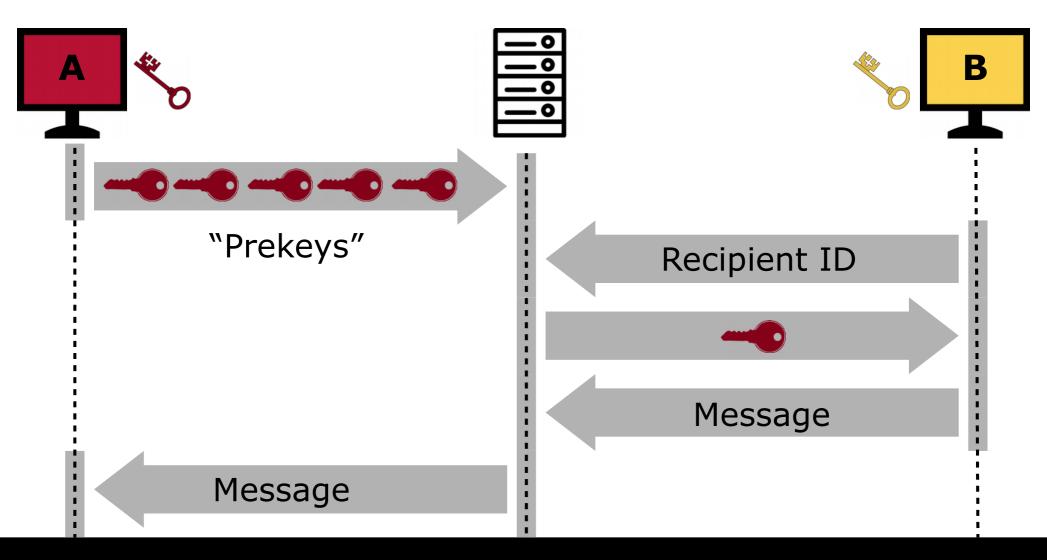
DAKEZ: Online Deniability



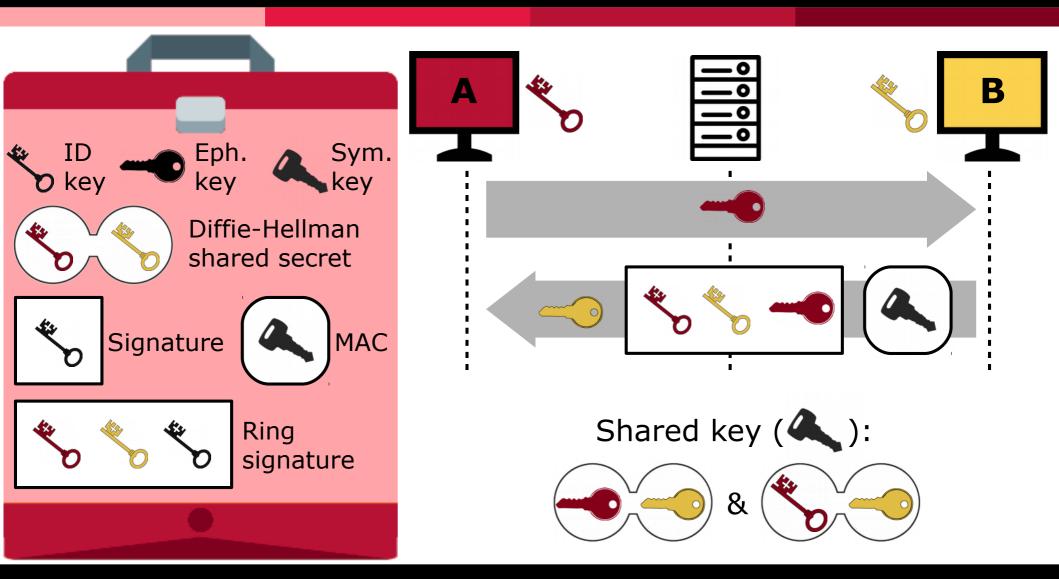
Mobile?



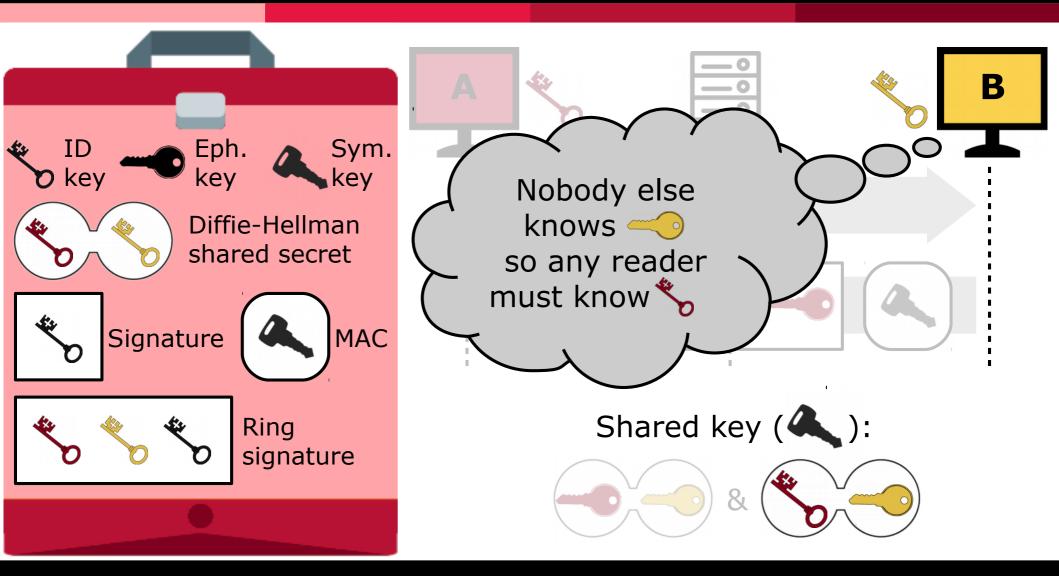
Mobile Use





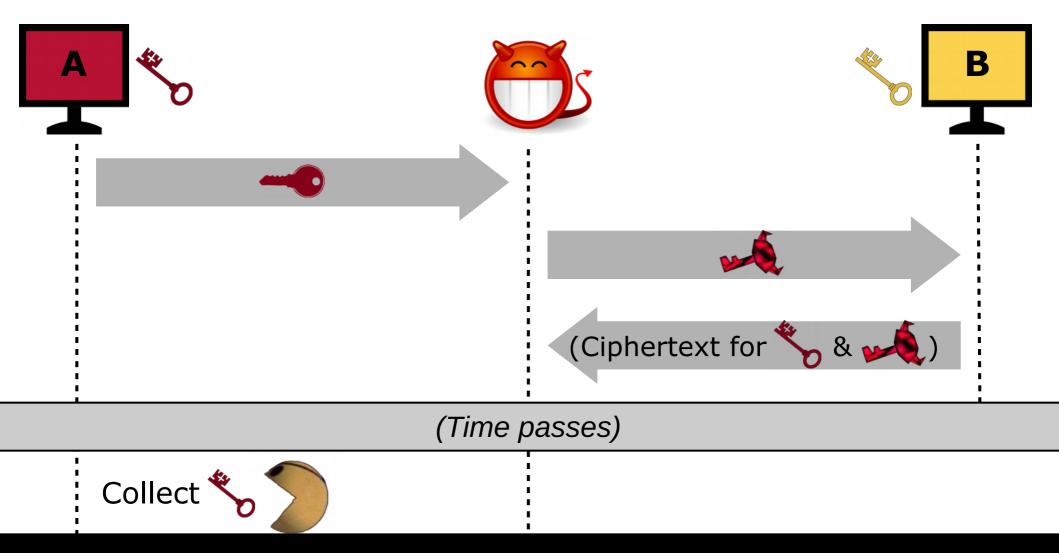


ZDH: Authentication

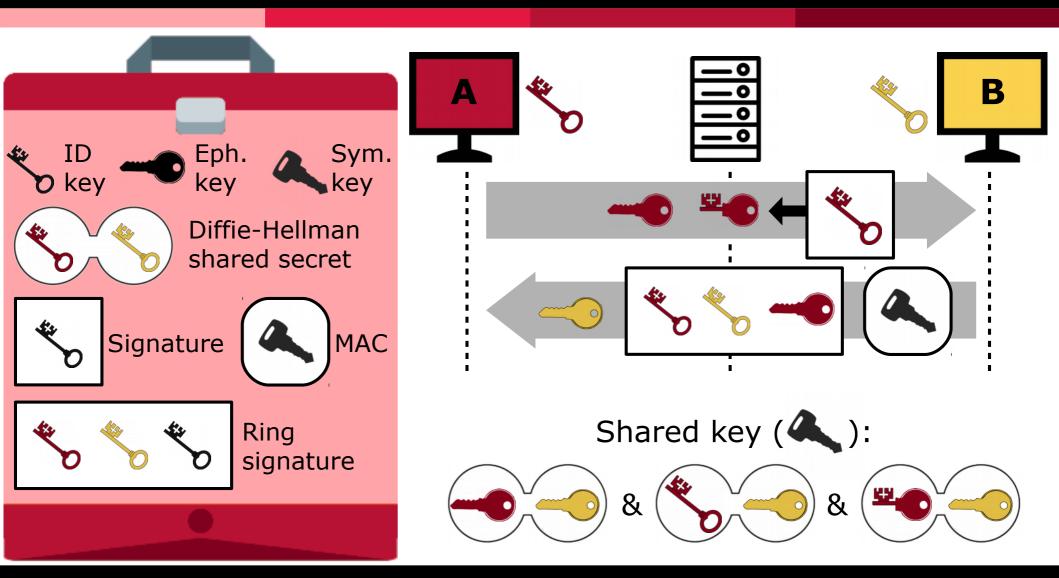


Weak Forward Secrecy

(Like Signal, originally)







Is This Secure?



Is This Secure?

										T			
													inverse of Strangly Deviation Andrewisation Key Dealarges for Steas σ Messaging mass -33
A Onli	proto	duard by	frank is solit in	other me		diven o					T). Key er	A ddays dd	
in this wor	the st provide	polynomi vantago k	defined a ring requivalent to (not repro- table were	talities up) t		ea pr	tire Reco	nd lif (s		is uncorru identifier	the flow to A with flow	pi — if A has previously computed P ⁽⁰⁾ , thus S must have – the electric mass against to J.
in an abstr tions. This	allosi putie	1. The a data 4	with more set	mitions for the the c			a DEP theo aplat size				distinguisi Offline d	any of the m to delaying (components to should notice computed by JD. a low Since DSir is understable with moment to insider
attado-m	NE NE NE NE	2 1 t d	lonelivad pa	Caret	original	ts osta the	ir co Dor	d De Brace	od Core		2 Office of the start and it in this new S officers S		in this case, S rations $S_{K=0}$ if from $G_{K=0}^{23,N23}$ using commution, it is only non-life to much this state if $J^{(2)}$
													terprom ed Strangly Deckal e An & retina ind K ny Drahargen for Stean = Mennaging anno 405
E.7	est arctine effectively	\mathcal{F}_{ipp} and \mathcal{F}_{res}	$G_{\text{terms}}^{\text{dynamed}}$, and to model th	sugar to T to $\mathcal{F}_{lense in}^{\prime}$	F.5.8 Co When As	mation, a to the one	Algorit	this ma- tor care	that reev ity under	Algorith	Algorithm		and $\delta x = in$ Section G.1. S computes $\kappa =$ Although ϕ now contained ongetermainformation— $KDW(\delta(g^{*})^{*} (g^{*})^{*} (g^{*})^{*} (g^{*}) ^{*}M_{B} = KDW(\phi), g^{*}$ and its signature (—there values do not help Z to
We n ou F	if hot distinguis	tane ago i establis	F.3 Proc	to involue S stude (S compt	spat to sesions d	on (inc Gene	n care trea i cadio tina	posible à shandhe	puted by	on (inc. eò Ganerati		and then reaces $MAC(M_0, t)$. distinguish between S and A , S more exitent $M^{(0)}$ denks the validity of the signature $ t \leq s$ leaves the
DAIK of A i	suger, and	si sand a tor	F_3 Proc	to indirect	name. If y outputs t	bound to	Cang Cang		sible (doe	retrieve tion, it al	Canpab Canpab		M.4.3 Receipt of ψ_3 by uncompared $I^{(4)}$ — service in the same memory as a real responder. If Z m-
proto them	the output	notify \overline{R} finish m	Theorem	(inc, sid, \overline{J} , valuely send	tics. In a bistorical	IND-CCA it is also a	Late Cang	G.1 S	and the la group) if,	on (opie- if (up)	Lat t = " Compate	11	This can is mostly the same as the can from Sec. plays a signal poly α generates an from a compt of tion G.1 with two differences. Heatly, when chains: $\overline{I} \le \frac{2}{3} \frac{MLDR}{M}$, S still effectively simulates $k^{(0)}$ boundly.
i sadin t	absonat a in all	party P, i then R)	if the Di- ours, the	 Otherwise, ing a siple 	A M molicita	vents ,4 fr sessions to	Cang	copt the	boarst ga the "part	if CP is if (top)	Caspab	2.0	ing that ψ_1 metabols the ψ_1 message and by $f^{(0)}$, its physical the signed proless or studied a correspond one S first ratio as the latest signed polesy for T by absorbes not effect the security properties of the MAC.
si nant. Li negra	termory a domestic	stasion kr plishthis	kay rapo comptio	discosing the plantext or	manivad a mandora a	out corrup the siplar	Sead	G ^{apters}	constitution by a correspondence of the second seco	$r \leftarrow \{0,$	Compete Send (in	14G., 1	sending (q_0 = securities, \overline{I}) to \overline{G}^{NLOS} , and marking or proof in ϕ_i . ($q_0, \overline{I}, \overline{g}^{(i)}, \overline{\xi}$) in response if $\overline{g}^{(i)}$ was the signal parks. Windly S sho shorts \overline{I} when ϕ_i includes an out-
E.7.1	posibly a party is a	for not see protoe de	dailying (prade on	strady a		Loral Bak	G.11 F	sibly care	Record	Locally : Malt	orat	transmitted in ϕ_1 and $\overline{g}^2 + g^2$, then S tructs ϕ_1 as dated \overline{g}^2 when $6.n$. This refinited the signed prokey
White a	tana ara in	tion[49])	within the tive second	will discuss large for M ⁴	provide B IZ,4 a	G Pro It is possi		for the - If J ^{CA}	H Pro	on (opio- lif (up t		-	ity of many, S much (verify, $\{g^{\Gamma}, g^{J}\}, t, many$) to N , viewly the behavior of a real initiator, who always knows
A tion (parties an	F_{ipp} and $ure = 0$	onale AS	$\gamma = 1000$ S then p	almady n provide ti	man nyi	K DF ₁ , i modul t	might The s	H.1 Fo	if (P is if (top)	$a_{2}^{\Gamma} = a_{2}^{\Gamma} a_{2}^{\Gamma}$		where $\log t = T^* \ ^2 M' \ g'\ _{H^2} \ Q_{J}\ _{L^2}^2 \ \Phi_{J}$ which signal proton using an did key.
ha ga	E.J.S Da Since set	$\mathcal{F}_{dpop,limin}$	Note that yerseries de	"1" "B" g' produces th	F.6 Pro	most prop ideal. fram	The to the o	constant.	ân	ikmond on (opin-t	Although , the simula	Na	H.5 Proof of Indistinguishably
with signer	EUC nod formation	inputan sion key t	whereas the adaptive ad	 - if S principal molicit 	The prod	Spawn' in Section	iterty is video as	 Other prode 	We provid scorecy, a	if (top) Sead	prology so		The proof of indistinguishability given in Section G.2 also applies here with second additional emactics.
in s. r raing	No inform sist of set	to \mathcal{F}_{ipopl}^{i} time tops	The con- identical to	g^{r} and η	described ory states	monity to Theorem	for the	"1" []" ing th	the forwa electry dist	} olso -	H2.1 Fas	wow.	The section keys produced by indices N_{XZW} and N_{ZW} continue to be indictinguishable to Z due to the
b man	is grant	ing form	criminating locify or	proof m	F.6.1 Th	if the A	ideal for relation	to for - if	from the	Sead }	3.2 DH offi- twees the		CD00 eccomption for 6, when the inputs to ED07 still include terms that 2 moment compute the inclusion of
produ the la	ψ_2 and ψ_2 contents of	$\mathcal{F}_{\text{ipop-limit}}$ and (y, \overline{R})	simply hore	(prove, 1 a move, 1	This site	might at the star of the star	АЦ _О 2106, ч	nol	scorecy in the proof	on (opie-o if (CP	in the cost be represent	t in	$g^{\Gamma \nu}$ does not negate the computational independence of the random model's outputs.
ii to Z	insider og dore net s	like \mathcal{F}_{pent}^{+} most not	\overline{R}_i rating SA non-inform	 - if \u03c6₁ we must to \u03c8 	M ^{CO} castil ungo flore	ra past suapti	den rasing Algorith		forward a with \mathcal{F}_{m}^{i}	if ((P	and a part	tun	
abort	the species	brook for word som	intheproof structure as	standing a N. Sing	located by	GLC-n Istaid	the pro- also ad	npi to	brook stra	lif (top) Sead	gnish e fr ropt of boil	lam i	
in the to the	F Pro	protond b Looking a	identical to to the DAK	seads the protect of	tion), Z full lay r	insPro-	varify a	10.4 (20	naangta in distinggale	3	S shorted) on opt-red	fire	
v noin	in this up As in Ap	Spawa' a natista th	F.4 Proc	to be as	some forg tional 160	There are The cross	exclusion set of an	- 10.0	Franklin in	$\mathcal{F}_{lamp,lints}^{i}$	ity def ing forwar		
sation genera	Section F	F.2 Sp	(Skatak) TI	receieve	that they	prosiedore generation	that an r, as pa	N	informati	Algorithm distributi	is to show low $Pt = x_{NR}$		
identi bio se	with our	We might	App make i that execut	ning o _A Cisto y to	F.6.2 At	toma som	couly the It is	san Sin the	deliver (good has 0 When a	scorecy the men with	it s	
contpo read p	stations d	terface 1	while inter- flow of Spat	S then would would (net-los	This sites by A in t	randoles es ports add	usin, do- the inte	the second	kay was g azata are	Theorem	order to p dom orade	in N	
these the p	F.1 Ide UGE da	the group the appro-	the second Section	record a share key. If insiPro-	setana der i no in Sout	We define to mean t	,64 is a Oxford o	its wit	nets N _Q	if the 2 mp-all	sage size.	th.	
gyaish	based star	partine re shared for	and Station	the last Other N if J ¹⁰⁰ is an	mation of movings a	only correctly \mathcal{F}_{pup}	also not note o la	tanis tani	statisty, 5	appined appeal to	apic-retris (∉) ^F . How	nn	γΔς ΙΙ
é soa K Die	slity rand same prof	tation opposite	F.5 Sim	uncorrupted.	tivity spa from M ⁽⁴⁾	may not a party. In	output (10 I	institute is contained	tion la GUC-n	then there thereby sol		"Yes."
che in Cittat	connect by cally, \mathcal{F}_{ip}^{loc}	mapondar Wei d	F.5.1 Gene As in Section	F.5.5 Receipt	nation. J RSigista	transmit a This moto	without to KDF	Cirvan	teerfol, eve Theoryme	lightid Builting	H.3 Pro	of	
to 🙀	tivmes. I	G ^{arana} , i tion fran	dalays mea	When means to be from J*	F.6.3 Als	to GUCs	to easy knowled	As in S_{1} it to $J^{(1)}$	and 2008 If Spa	There are	(Skutshi) T		
	a twoffes straight o	11 This at	when A ro- and replicat	broadcast a m ignered S the	This sites	tionality (it came	11 11 1	array the issue insta	Theorem, the use of	the proof of we only hig	g dali	
	depicts th	proof sheets reacted roots		5, and the pro-	by Aint	first three	posed		ontput hy	shown in	tion between	-	
												1	
												1	

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

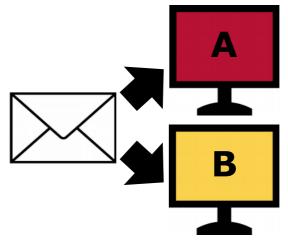
Extras in the Paper



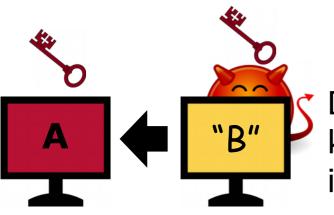
Extras in the Paper



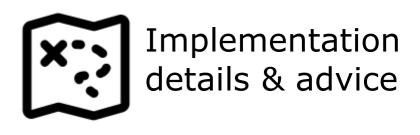
Quantumresistant transitional security



Efficient dual-receiver encryption



Defeating key-compromise impersonation



Summary

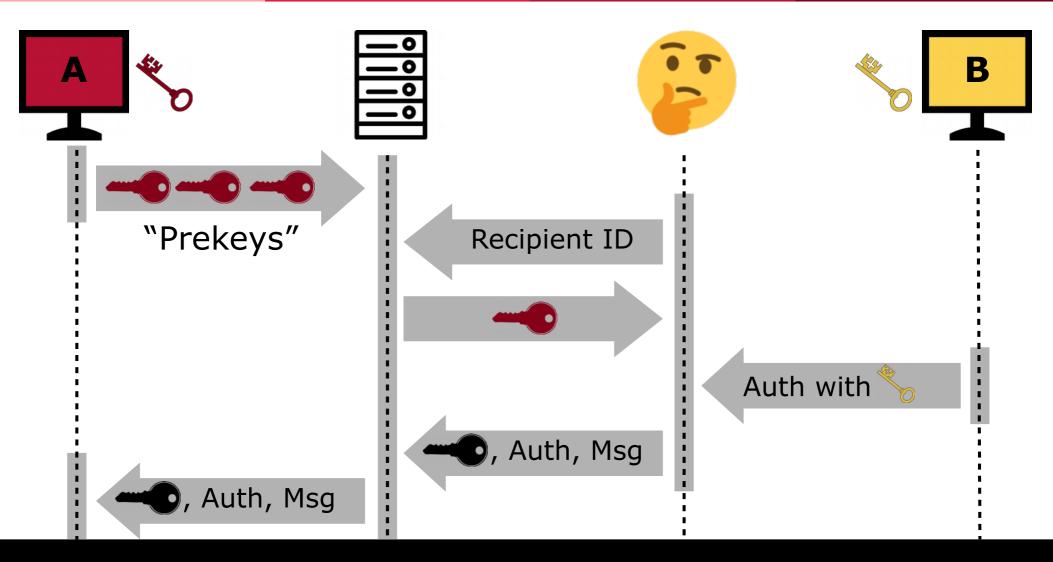
- New key exchanges: DAKEZ, (X)ZDH
- Secure connection, eponymous, no all-verifier authentication required? Use these!
- Code & data: crysp.org/software/dakez_xzdh
- Come see OTRv4 at HotPETs
- Coming soon: group messaging

Thank you! njunger@uwaterloo.ca



You've Activated My Bonus Slides!!!

Limited Online Deniability



RSDAKE and Spawn

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

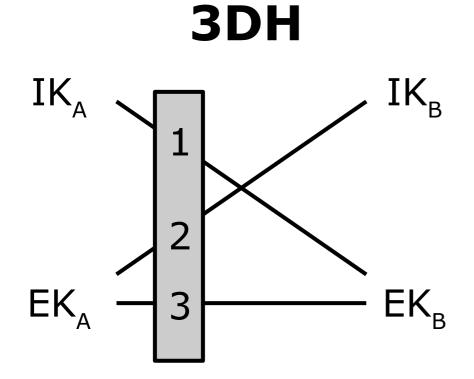
DAKE Comparison

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

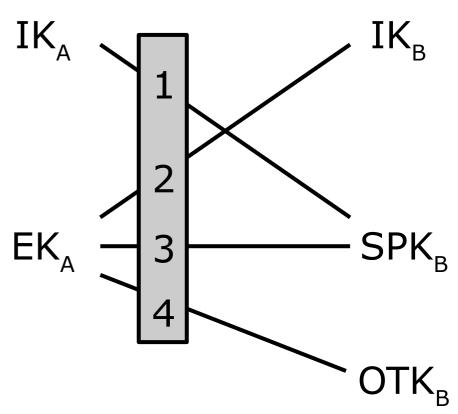
	ECDH	3DH	X3DH	SIGMA-R	Φ_{idre}	RSDAKE	Spawn	DAKEZ	Spawn ⁺	ZDH	XZDH
Offline Deniable	•	•	0	0	•	•	•		•	•	•
Online Deniable	•	-	-	-	•	•	0	•	0	0	0
Authenticated	-	•	•	•	•	•	•	•	٠	•	•
Non-Interactive	•	•	•	-	-	-	•	-	•	•	•
Forward Secrecy	-	-	0	•	•	•	-	•	-	-	0
Proof Model	SM	ROM	ROM	ROM	SM	SM	SM	ROM	ROM	ROM	ROM
Public Key		0.0228	0.0240	0.0240	0.40	206	206	0.0440	0.0429	0.0441	0.0444
Generation [ms]	-	(0.0012)	(0.0013)	(0.0012)	(0.01)	(8)	(4)	(0.0016)	(0.0016)	(0.0018)	(0.0017)
Exchange [ms]	0.1733	0.4229	0.5533	0.3478	13	6 6 3 0	3 390	1.094	1.3683	0.778	0.9217
	(0.0033)	(0.0050)	(0.0056)	(0.0048)	(2)	(50)	(20)	(0.014)	(0.0082)	(0.013)	(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 1 4 0	7 598	73763	464	512	304	304

• = provides property; O = 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



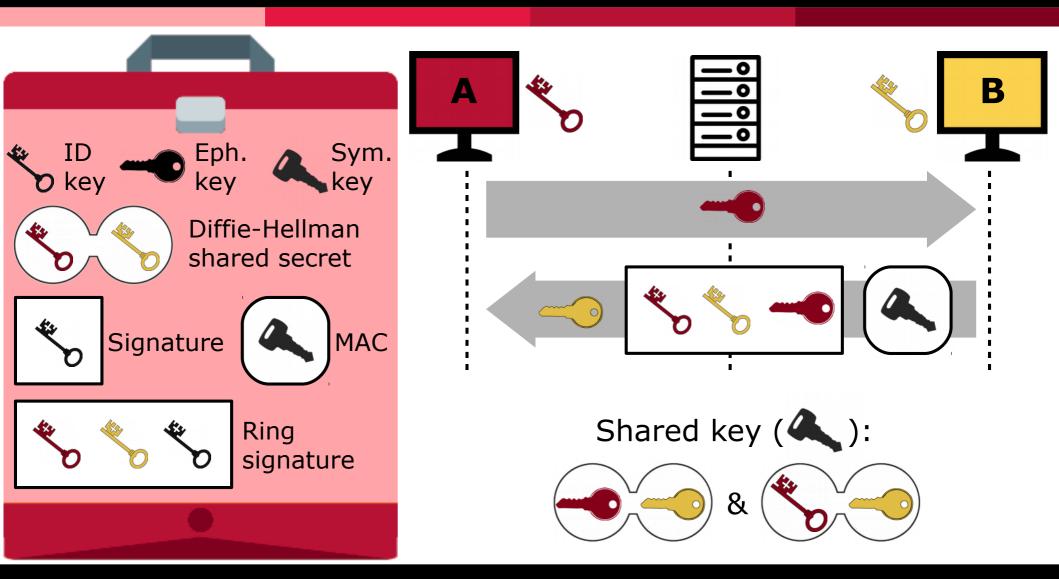
X3DH



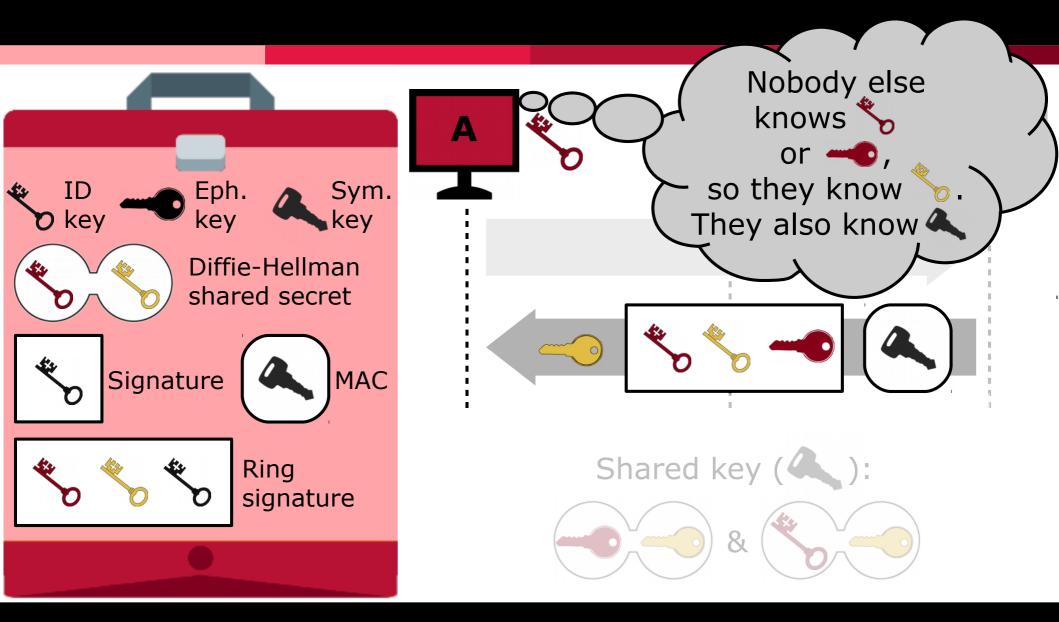
Lack of Contributiveness

- **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

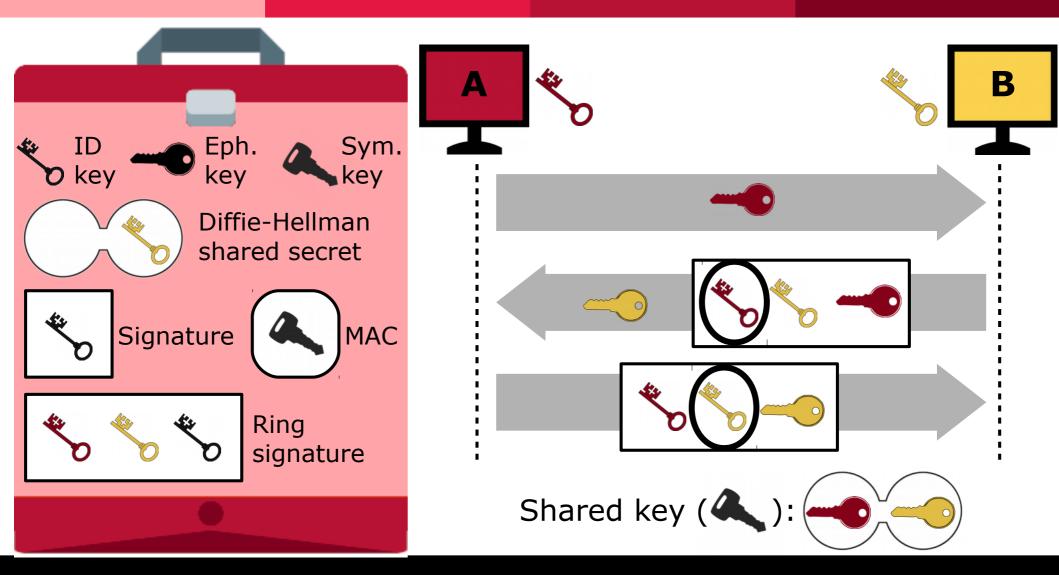




ZDH: Authentication



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



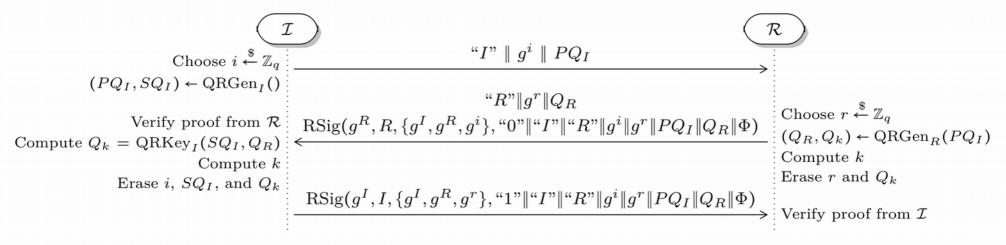


Fig. 2. The DAKEZ protocol. Φ is shared session state. The shared secret is $k = \text{KDF}(g^{ir} \parallel Q_k)$.

ZDH & XZDH

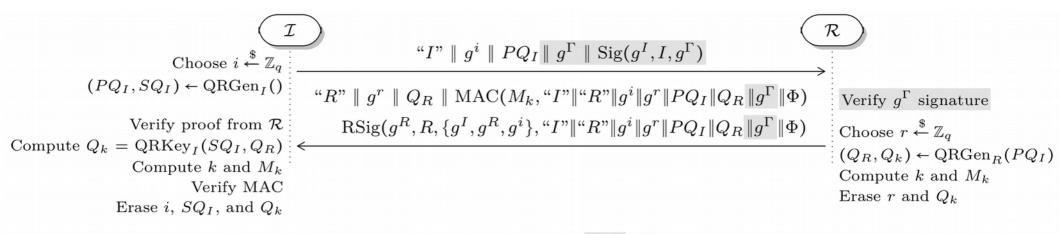


Fig. 4. A ZDH/XZDH exchange. Φ is shared session state. $\kappa = \text{KDF}_1(g^{ir} || g^{\Gamma r} || g^{\Gamma r} || Q_k)$, $M_k = \text{KDF}_2(\kappa)$ and the shared secret is $k = \text{KDF}_3(\kappa)$. Shaded terms are used in XZDH only, and omitted for ZDH. In XZDH, g^{Γ} is a reusable signed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