QUANTUM KEY DISTRIBUTION IN THE CLASSICAL AUTHENTICATED KEY EXCHANGE FRAMEWORK

Michele Mosca[1,2] Douglas Stebila[3] Berkant Ustaoğlu[4]

Institute for Quantum Computing and Dept. of Combinatorics & Optimization
University of Waterloo, Waterloo, Ontario, Canada

Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada
mmosca@uwaterloo.ca

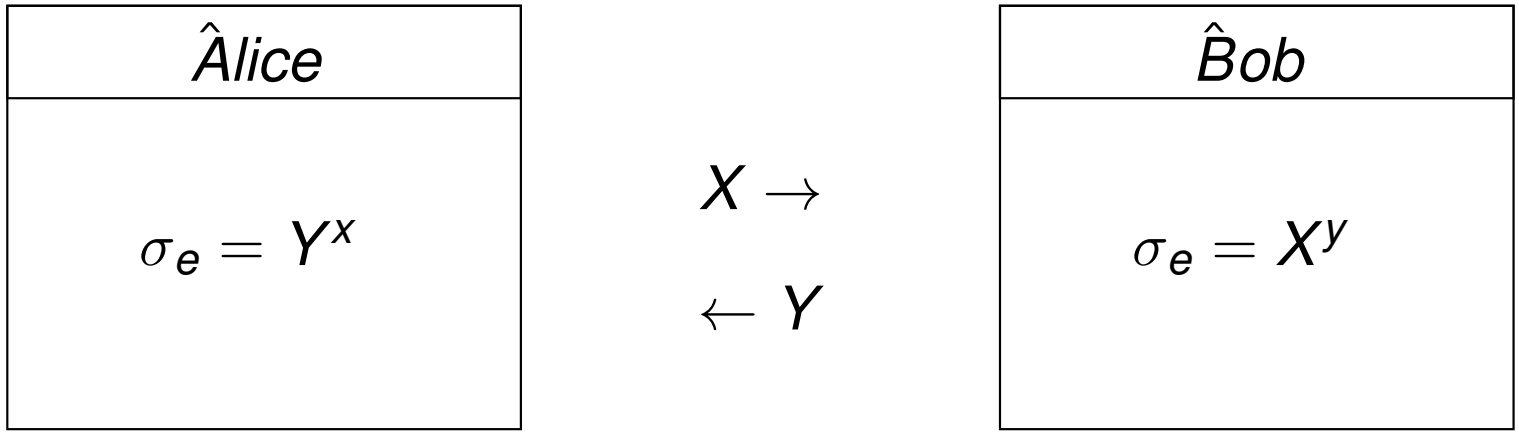
Information Security Discipline, QUT, Brisbane, Queensland, Australia
stebila@qut.edu.au

Department of Mathematics, IYTE, Izmir, Turkey
bustaoglu@uwaterloo.ca

Agenda

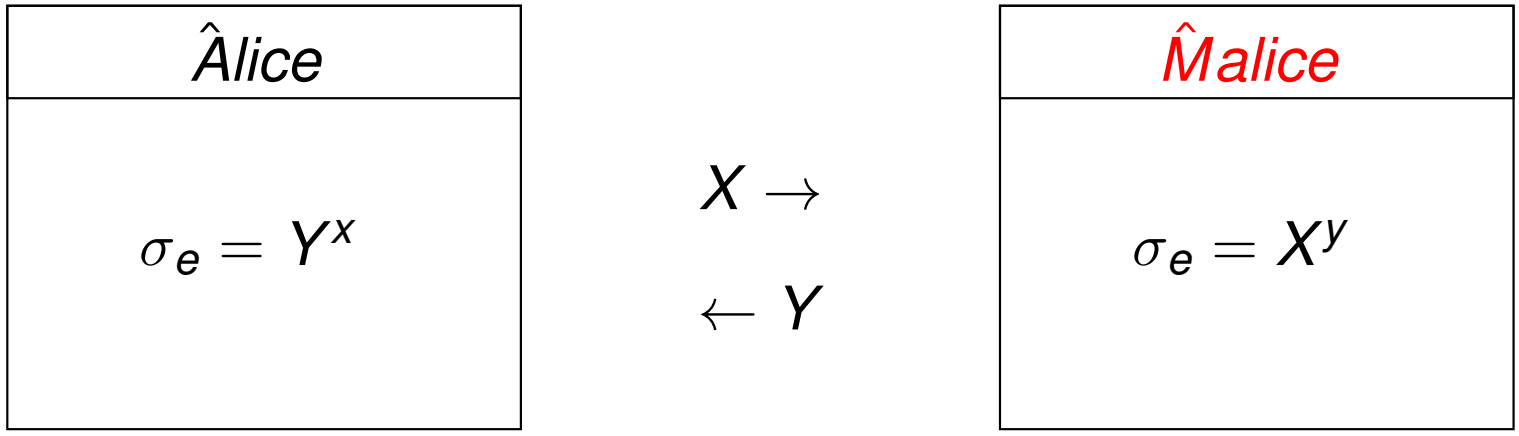
1. classical definitions and motivations
2. quantum protocols
3. our view
4. further considerations

Idea Diffie-Hellman



$$\kappa = \mathrm{H}(\sigma_e)$$

Person-in-the middle



$$\kappa = \mathrm{H}(\sigma_e)$$

Authentication

$\hat{A}, a, A = g^a$		$\hat{B}, b, B = g^b$
$\sigma_e = B^a$	$X \rightarrow$ $\leftarrow Y$	$\sigma_e = A^b$

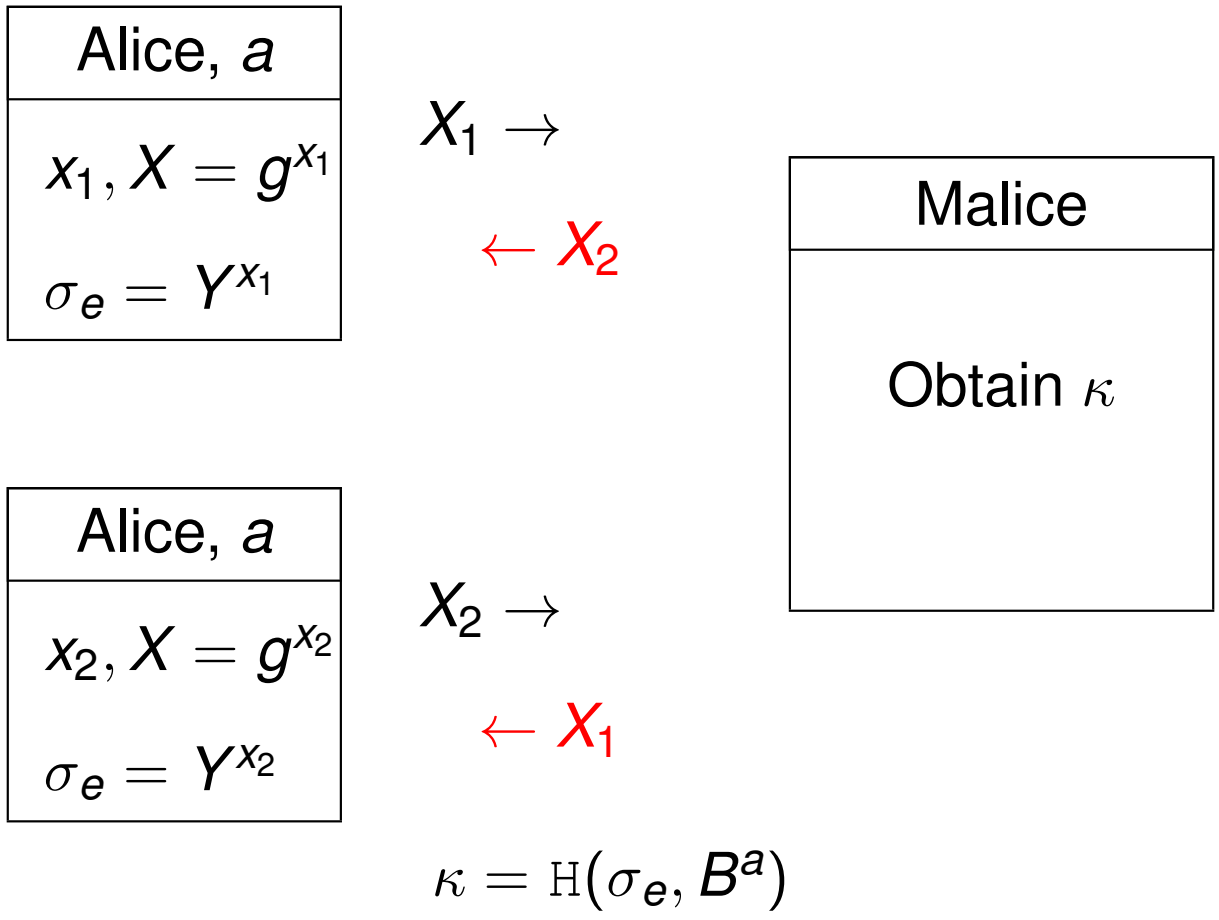
$$\kappa = \mathrm{H}(\sigma_s)$$

Unified model (UM) protocol

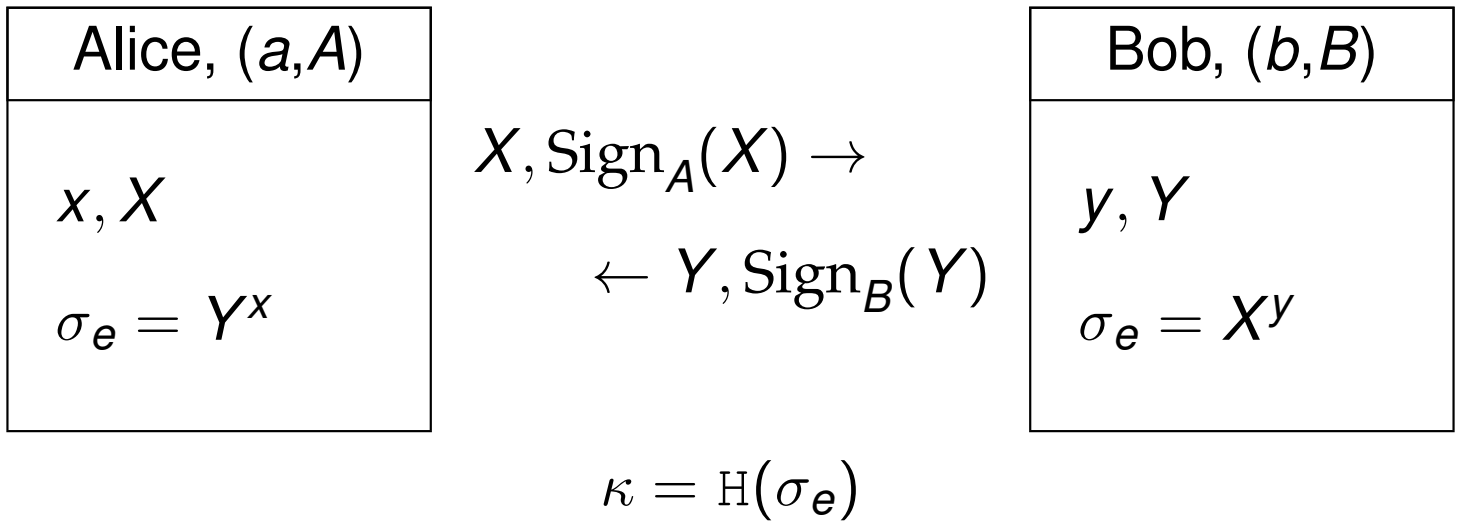
Alice		Bob
$a, A, \sigma_s = B^a$	$X \rightarrow$	$b, B, \sigma_s = A^b$
$x, X, \sigma_e = Y^x$	$\leftarrow Y$	$y, Y, \sigma_e = X^y$

$$\kappa = \mathrm{H}(\sigma_e, \sigma_s)$$

Multiple sessions



Signed Diffie-Hellman



MQV

$$\mathsf{D} = \mathrm{H}_e(X) \qquad \mathsf{E} = \mathrm{H}_e(Y)$$

$$\kappa = \mathrm{H}(\sigma)$$

$$g^{(x+\mathsf{D}a)(y+\mathsf{E}b)}$$

UKS on MQV

$\hat{A}, a, A$		$\hat{M}, m, M$		$\hat{B}, b, B$
$\underline{s : \hat{B}, x, X}$	$X \rightarrow$	$Z = XA^{\mathsf{D}} g^{-u}$	$X \rightarrow$	$\underline{s : \hat{M}, y, Y}$
$\sigma = (YB^{\mathsf{E}})^{x+\mathsf{D}a}$	$\leftarrow Z$	$\mathsf{P} = \mathrm{H}_e(Z)$	$\leftarrow Y$	$\sigma = (ZM^{\mathsf{P}})^{y+\mathsf{E}b}$
		$m = u/\mathsf{P}$		

$$\mathsf{D} = \mathrm{H}_e(X) \qquad \mathsf{E} = \mathrm{H}_e(Y)$$

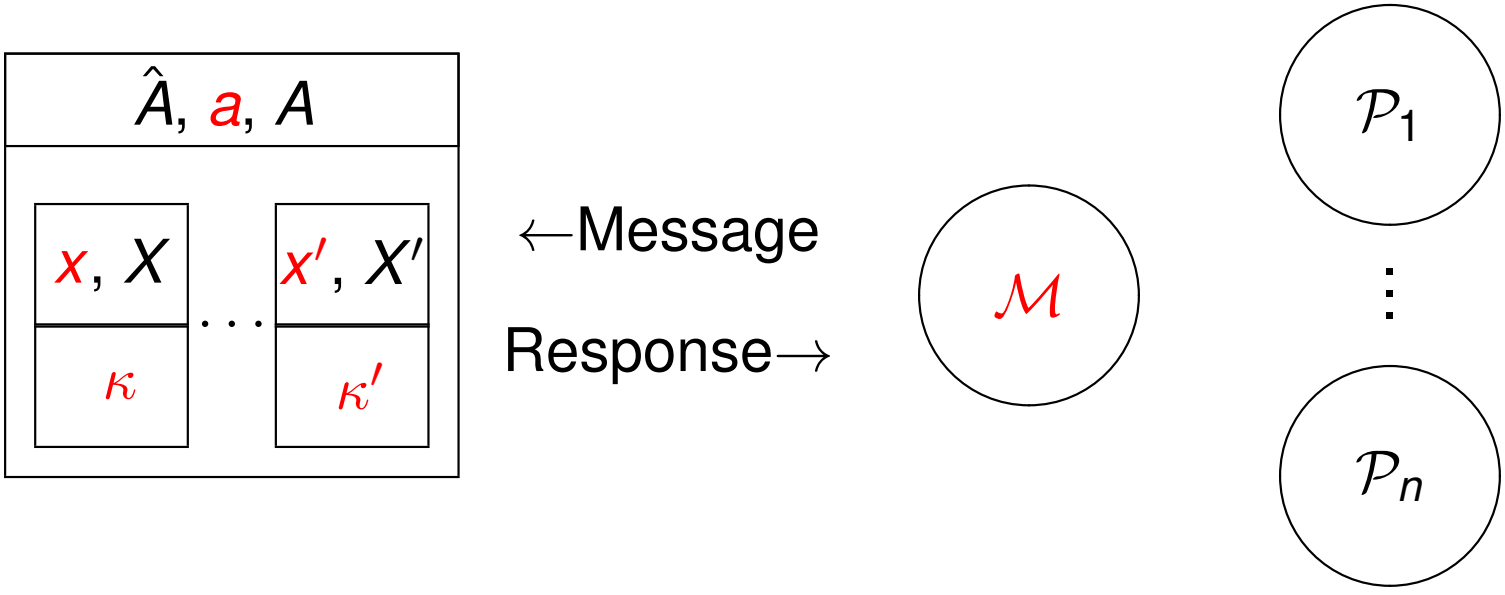
$$\kappa = \mathrm{H}(\sigma)$$

$$ZM^{\mathsf{P}} = XA^{\mathsf{D}}$$

Problems overview

- Person-in-the middle
- UM concurrent sessions
- signed DH ephemeral keys
- UKS on MQV

Model basics



$$b \in_R \{0,1\}, \qquad \kappa_b = \begin{cases} k_{test} & b = 1 \\ k_R & b = 0 \end{cases}$$

Models comparison

	BR/BJM	CK01	eCK
Communication	yes	yes	yes
Static key	yes	yes	yes
Ephemeral keys	no	yes	yes
Session keys	yes	yes	yes

QKD models

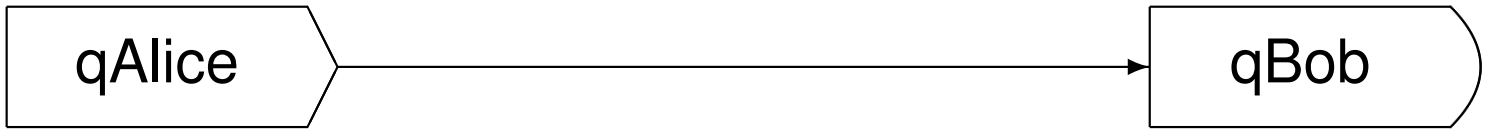
stand alone

- two parties
- authentication for granted

UC framework

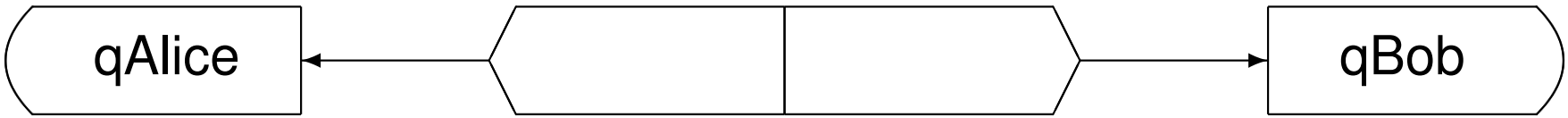
- no information leakage
- information-theoretic authentication

Prepare-send-measure (BB84)



- long-term authentication key
- basis bits
- data bits
- information reconcilation randomness
- privacy amplification randomness

Measure only (Ekert91, BBM92)

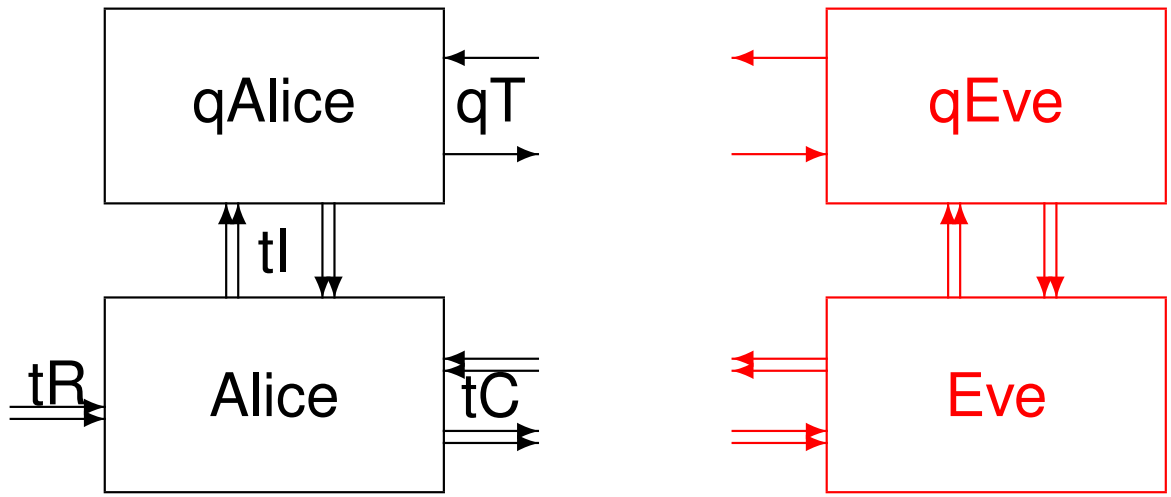


- long-term authentication key
- basis bits
- information reconcilation randomness
- privacy amplification randomness

Send only (BHM96, Ina02)

- long-term authentication key
- basis bits
- data bits
- information reconcilation randomness
- privacy amplification randomness

Unifying frameworks



Freshness

$$\left(\kappa, \hat{B}, \left[\begin{array}{c} \left(\begin{array}{c} X \\ A \end{array}\right) \\ \\ \left(\begin{array}{c} Y \\ B \end{array}\right) \end{array}\right]\right) \quad \left(\kappa, \hat{B}, \left[\begin{array}{c} (s^A_{dAB}) \\ \\ (s^A_{bAB}) \\ \\ (s^B_{dAB}) \\ \\ (s^B_{bAB}) \\ \\ (s^A_F) \\ \\ (s^A_{P,G}) \end{array}\right], [(pk_A)]\right)$$

$$\kappa = g^{(x+\mathrm{D}a)(y+\mathrm{E}b)}$$

Adversarial goals

short term Active adversary

- t_c classical runtime
- t_q quantum runtime
- m_q quantum memory

long term Passive adversary

- t_c, t_q, m_q output
- bounded by physics

Protocol comparison

Protocol	Signed Diffie–Hellman CK01	MQV style	BB84 BB84	EPR Eke91	BHM96 BHM96,Ina02
Protocol type	classical	classical	quantum prepare-send-measure	quantum measure-only	quantum prepare-send-only
Security model	CK01 CK01	eCK LLM07, this paper	this paper	this paper	this paper
Randomness revealable **before** protocol run?	× static key × ephemeral key	at most 1 of static key, ephemeral key	× static key × basic choice × data bits × info. recon. × priv. amp.	× static key × basis choice × info. recon. × priv. amp.	× static key × basis choice × data bits × info. recon. × priv. amp.
Randomness revealable **after** protocol run?	✓ static key × ephemeral key	at most 1 of static key, ephemeral key	✓ static key ✓ basis choice × data bits ✓ info. recon. ✓ priv. amp.	✓ static key ✓ basis choice ✓ info. recon. ✓ priv. amp.	✓ static key ✓ basis choice × data bits ✓ info. recon. ✓ priv. amp.
Short-term security	computational assumption	computational assumption	computational or inf.-th.	computational or inf.-th.	computational or inf.-th.
Long-term security w/short-term-secure authentication	×	×	✓	✓	✓

Future work

- multi-party
- privacy
- pre-post QKD
- shared keys

THANK YOU!