RSAConference™2023
San Francisco | April 24 – 27 | Moscone Center



SESSION ID: CRYP-R02A

Multi-User CDH Problems and the Concrete Security of HMQV and NAXOS

#RSAC

Eike Kiltz[1], Jiaxin Pan[2], Doreen Riepel[1,3], Magnus Ringerud[2]

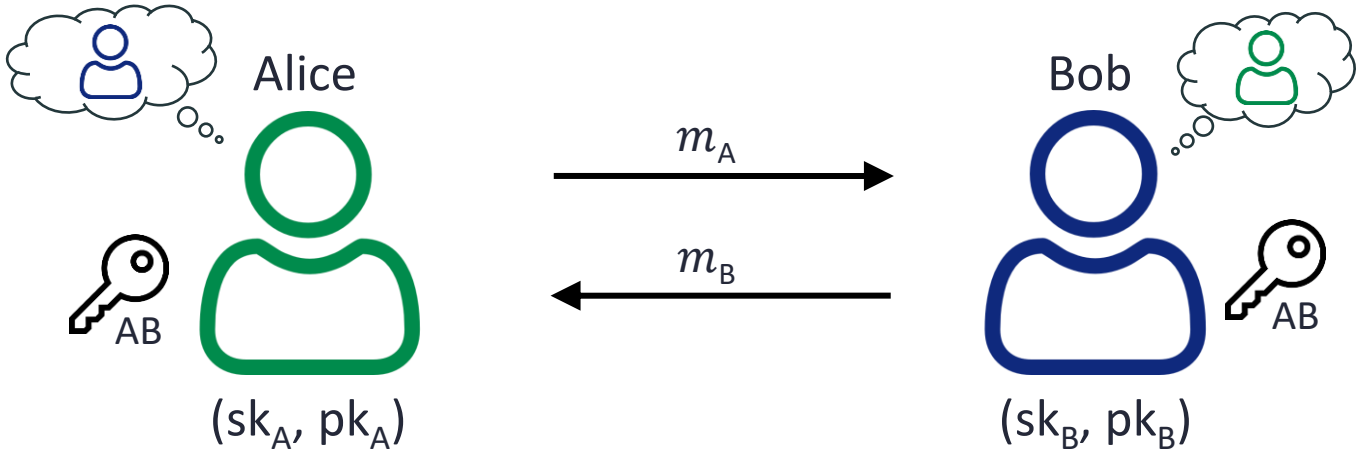
[1] Ruhr-Universität Bochum
[2] Norwegian University of Science and Technology
[3] University of California San Diego

Authenticated Key Exchange

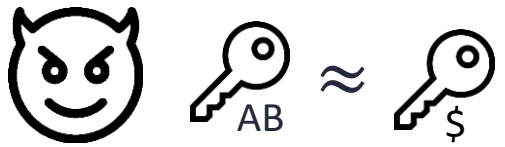
A cryptographic primitive with real-world applications

- TLS handshake
- Signal's X3DH key exchange

Goal: An AKE protocol allows two parties to agree upon a shared session key while authenticating each other.

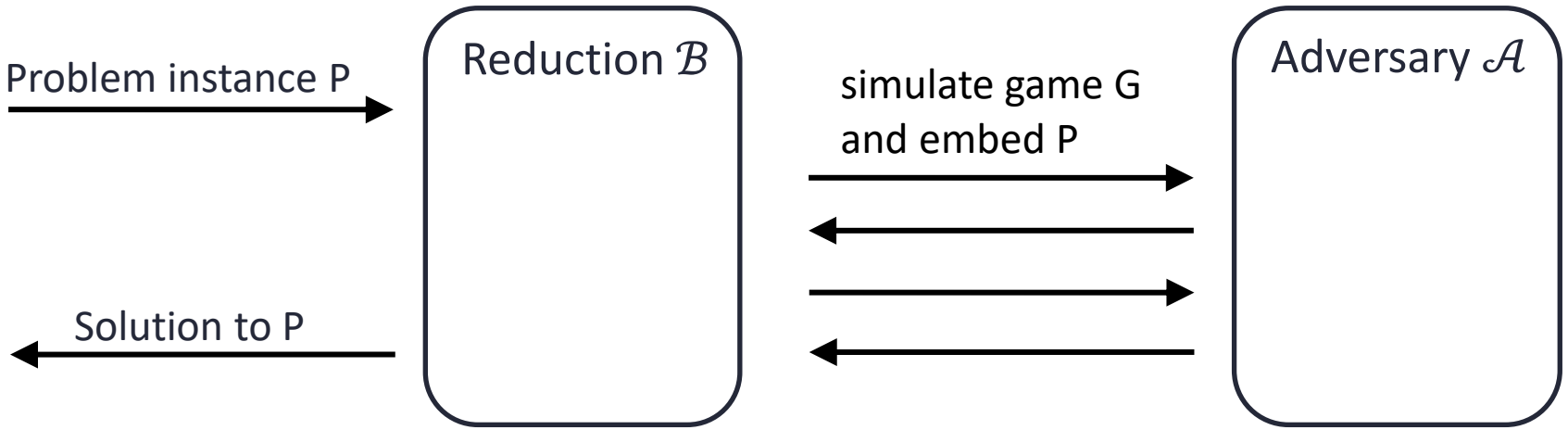


Game-based security:



Tight Security

We prove security of a protocol by a security reduction:



advantage $\epsilon_{\mathcal{B}}$ (solving P)
running time $t_{\mathcal{B}}$

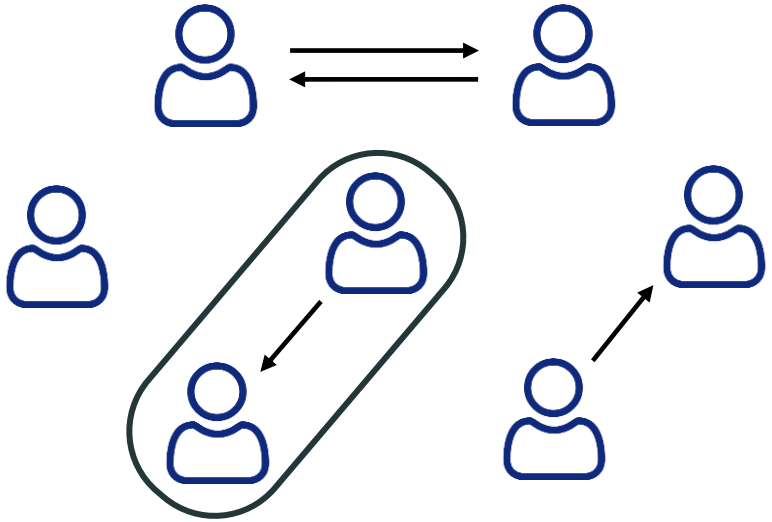
advantage $\epsilon_{\mathcal{A}}$ (winning G)
running time $t_{\mathcal{A}}$

Reduction is tight if $\epsilon_{\mathcal{B}} \approx \epsilon_{\mathcal{A}}$ and $t_{\mathcal{B}} \approx t_{\mathcal{A}}$.

AKE and Tightness

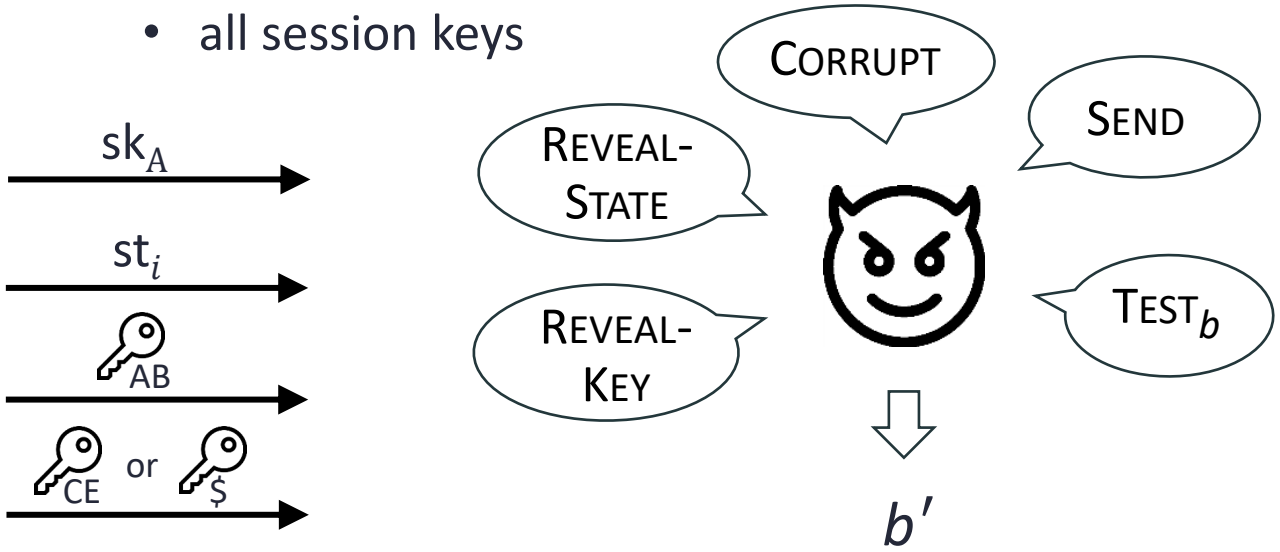
Security Game

- N users with key pairs (pk_u, sk_u)
- S sessions with session state (st_i)



The reduction must be able to simulate ...

- all secret keys
- all session states
- all session keys



Common Proof Strategy: Guess TEST session and make case distinction for corruptions

Many AKE proofs: $\epsilon_{\mathcal{A}} \leq S^2 \epsilon_{\mathcal{B}}$ ⇒ Increase parameters to compensate security loss

Tight proof? ⇒ Impossible for some classes of protocols

The HMQV and NAXOS Protocol

NAXOS

Alice $(a \in \mathbb{Z}_p,\ A := g^a)$

Bob $(b \in \mathbb{Z}_p,\ B := g^b)$

$x \leftarrow^{\$} \mathbb{Z}_p$

$esk_{\mathrm{A}} \leftarrow^{\$} \{0,1\}^n$

$x := \mathrm{G}(esk_{\mathrm{A}}, a)$

$X := g^x$ →

← $Y := g^y$

$y \leftarrow^{\$} \mathbb{Z}_p$

$esk_{\mathrm{B}} \leftarrow^{\$} \{0,1\}^n$

$y := \mathrm{G}(esk_{\mathrm{B}}, b)$

$d := \mathrm{G}(\mathrm{A}, X)$

$e := \mathrm{G}(\mathrm{B}, Y)$

$z := (YB^e)^{x+ad}$

$z := (Y^a, B^x, Y^x)$

$z := (XA^d)^{y+be}$

$z := (A^y, X^b, X^y)$

$$K_{\mathrm{AB}} := \mathrm{H}(\mathrm{A}, \mathrm{B}, g^x, g^y, z)$$

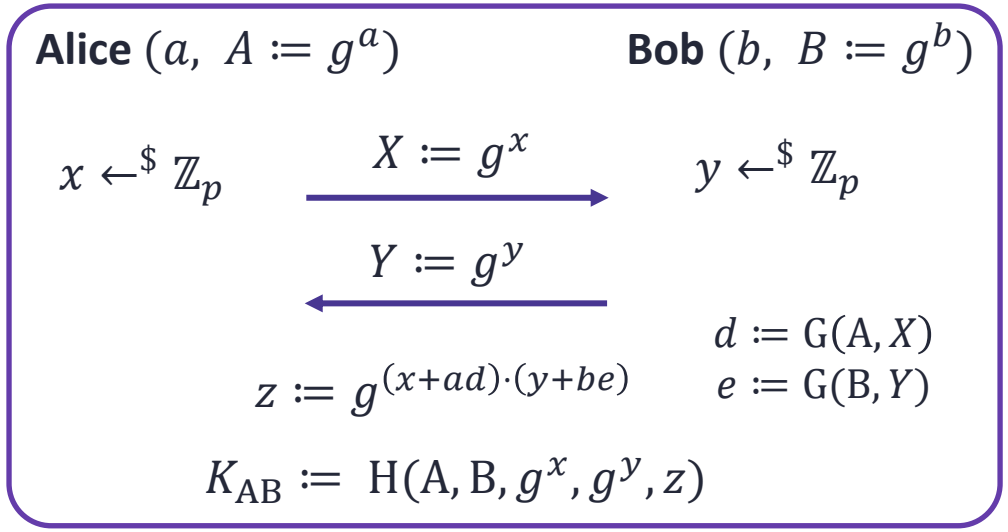
Our Approach

The Commitment Problem

- Answering corruptions vs. embedding the challenge
- Answering key reveal vs. test queries

The Generic Group Model (GGM)

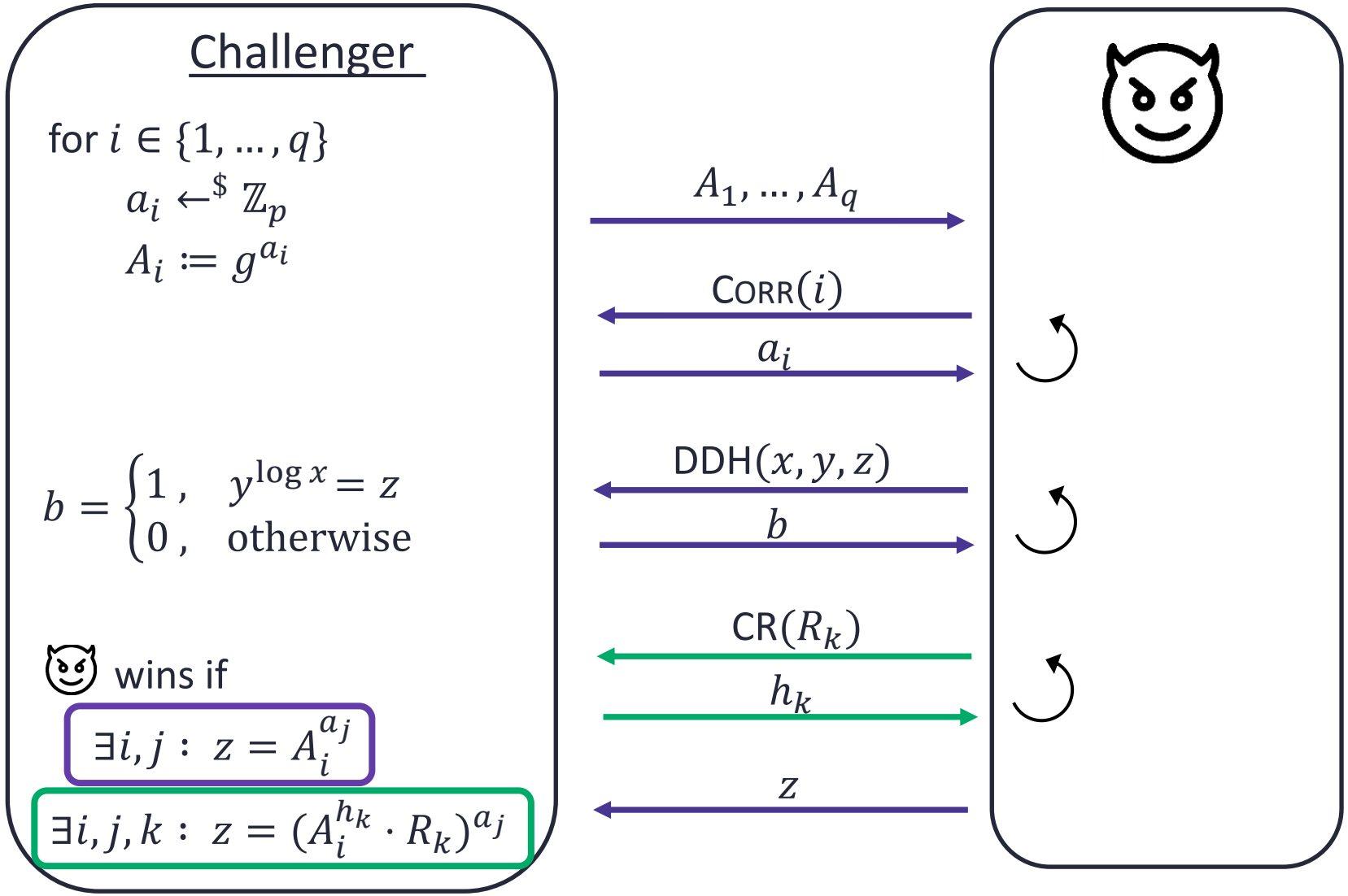
- Oracle access to group operations
- Goal: information-theoretic lower bounds for generic attacks



Capturing the Algebraic Core of the Protocol

- Prove tight security of the AKE based on variants of the CDH problem
- Provide GGM bounds for the assumptions justifying standard parameter choices

Multi-User CDH Problems with Corruptions



q-CorrGapCDH

⇩ tight

NAXOS

q-CorrCRGapCDH

⇩ tight

HMQV

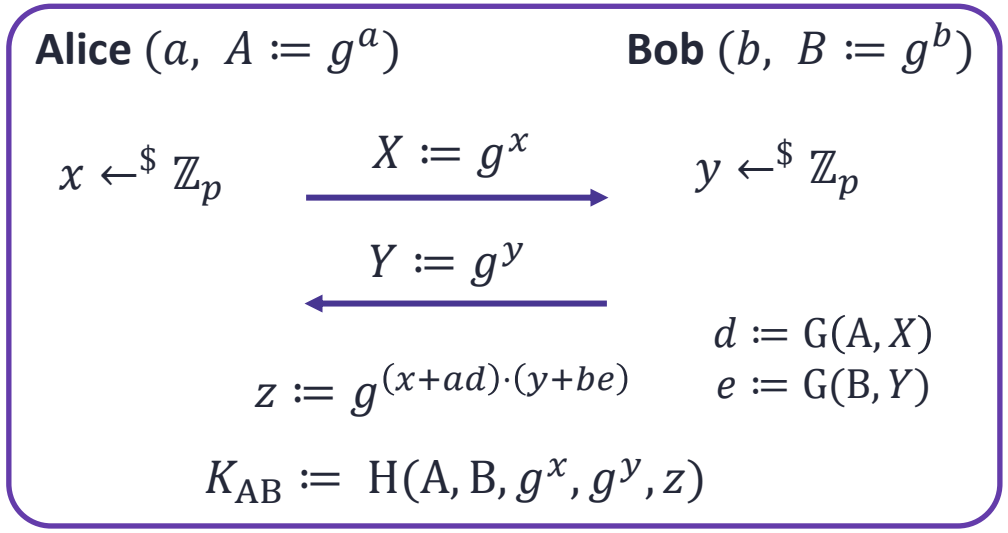
Security Proof

Theorem

HMQV is a tightly-secure AKE under the (N+S)-CorrCRGapCDH assumption and in the ROM.

Proof Idea

- The reduction gets as input $A_1, \dots, A_N, X_1, \dots, X_S$
- Use A_i as the i-th user's public key
- SEND query: Use X_j as message in the j-th session
- CORRUPT and REVEAL-STATE queries: use CORR oracle
- REVEAL and H queries: use the DDH oracle to check consistency
- G queries: get a new challenge using the CH oracle



➢ If $\mathcal{A}$ queries H on the correct value z for a tested session, we can extract a valid solution

Generic Bounds and Bit Security

Running time of $\mathcal{A}$: $t = t_{OFF} + t_{ON}$

- t_{OFF}: group operation and random oracle queries
- t_{ON}: number of users, sessions and test queries

Optimal GGM bound: $\frac{t_{OFF}^2}{p}$ (breaking DLOG)

GGM Bounds	ϵ_{old}	$-\log_2\left(\frac{\epsilon_{old}}{t}\right)$	ϵ_{new}	$-\log_2\left(\frac{\epsilon_{new}}{t}\right)$
HMQV	$\frac{t_{ON}^3 \cdot t_{OFF}^2}{\sqrt{p}}$	0	$\frac{t_{OFF}^2 + t_{ON}^2 \cdot t_{OFF}}{p}$	128
NAXOS	$\frac{t_{ON}^3 \cdot t_{OFF}^2}{p}$	32	$\frac{t_{OFF}^2}{p}$	128

$$p \approx 2^{256}$$
$$t_{OFF} \approx 2^{128}$$
$$t_{ON} \approx 2^{64}$$

Bit Security: if we target κ bits of security, we want $\frac{\epsilon}{t} \leq 2^{-\kappa}$.

Summary

Our Contributions

- Prove tight security of HMQV and NAXOS based on new assumptions
- Analyze these assumptions in the GGM to provide concrete bounds

Consequence: We do not need to compensate the tightness loss by choosing larger system parameters.

`ia.cr/2023/115`

Thank you!