

CS 258: Quantum Cryptography

Mark Zhandry

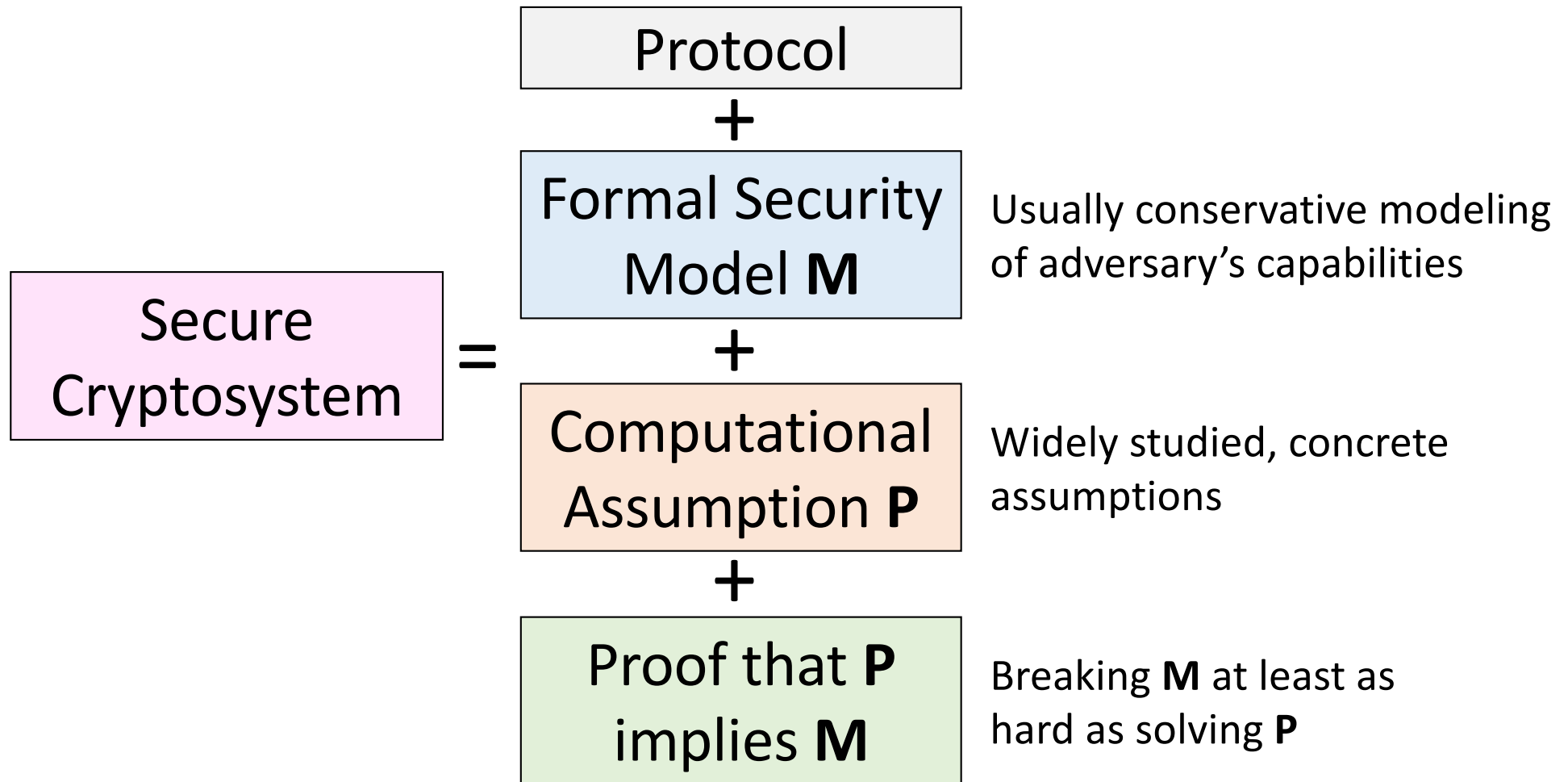
CS 258 so far

Quantum algorithms can break much of the crypto we use today

So we design new building blocks that
presumably resist these attacks

But, just if the building block is quantum resistant,
does that mean the applications are as well?

The Fundamental Formula of Modern Cryptography



Formal Security
Model **M**

Classically, typically of the form:

“For all PPT adversaries \mathcal{A} , there exists a negligible $\epsilon(\lambda)$ such that $\Pr[\mathcal{A}....] \leq \epsilon(\lambda)$ ”

Def (PKE, security): A PKE scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ is **classically** indistinguishable under a chosen plaintext attack (~~IND-CPA-secure~~, or just CPA-secure) if, for all **PPT** adversaries \mathcal{A} , there exists a negligible function ϵ such that

$$|\Pr[W_0(\lambda)] - \Pr[W_1(\lambda)]| \leq \epsilon(\lambda)$$

where $W_b(\lambda)$ is the event that \mathcal{A} outputs 1 in the following:

- Run $(\text{sk}, \text{pk}) \leftarrow \text{Gen}(1^\lambda)$, give **pk** to \mathcal{A}
- \mathcal{A} produces two msgs $m_0, m_1 \in \{0, 1\}^*$ *of the same length*
- Run $c \leftarrow \text{Enc}(\text{pk}, m_b)$ and give c to \mathcal{A}
- \mathcal{A} outputs an output guess $b' \in \{0, 1\}$

The “obvious” way to adapt classical definitions to the quantum setting is to simply replace PPT with QPT

Def (PKE, security): A PKE scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ is **quantumly** indistinguishable under a chosen plaintext attack (~~IND-CPA-secure~~, or just CPA-secure) if, for all **QPT** adversaries \mathcal{A} , there exists a negligible function ϵ such that

$$|\Pr[W_0(\lambda)] - \Pr[W_1(\lambda)]| \leq \epsilon(\lambda)$$

where $W_b(\lambda)$ is the event that \mathcal{A} outputs 1 in the following:

- Run $(\text{sk}, \text{pk}) \leftarrow \text{Gen}(1^\lambda)$, give **pk** to \mathcal{A}
- \mathcal{A} produces two msgs $m_0, m_1 \in \{0, 1\}^*$ *of the same length*
- Run $c \leftarrow \text{Enc}(\text{pk}, m_b)$ and give c to \mathcal{A}
- \mathcal{A} outputs an output guess $b' \in \{0, 1\}$

Computational Assumption **P**

Classically, typically of the form:

“For all PPT adversaries \mathcal{A} , there exists a negligible $\epsilon(\lambda)$ such that $\Pr[\mathcal{A}....] \leq \epsilon(\lambda)$ ”

The “obvious” way to adapt classical assumptions to the quantum setting, again is to simply replace PPT with QPT

Sometimes these assumptions will be false (e.g. DLog); in this case replace with suitable post-quantum assumptions

Proof that \mathbf{P}
implies \mathbf{M}

Classical proofs are a reduction, transforming PPT adversary \mathcal{A} for \mathbf{M} into PPT algorithm \mathcal{B} for \mathbf{P}

Classical reductions take classical inputs and produce classical outputs

If we feed a quantum \mathcal{A} into the reduction, will the output \mathcal{B} be anything meaningful?

Example 1: A case where things work out

Public Key Encryption from LWE

$$\begin{aligned} \text{pk} &= (\mathbf{A}, \mathbf{u} = \mathbf{A}^T \cdot \mathbf{s} + \mathbf{e} \bmod q) & \mathbf{s} &\text{ uniform in } \mathbb{Z}_q^n \\ \text{sk} &= (\mathbf{s}, \mathbf{e}) & \mathbf{e} &\leftarrow D_\sigma^m \end{aligned}$$

$$\begin{aligned} \text{Enc}(\text{pk}, m \in \{0, 1\}) &: \text{Sample } \mathbf{r} \text{ uniform in } \{0, 1\}^m \\ \text{Output } (\mathbf{v}^T &= \mathbf{r}^T \mathbf{A}^T, \quad w = \mathbf{r}^T \mathbf{u} + m \lfloor q/2 \rfloor \bmod q) \end{aligned}$$

$$\text{Dec}(\text{sk}, (\mathbf{v}, w)) : \text{Compute}$$

$$\begin{aligned} w - \mathbf{v}^T \cdot \mathbf{s} \bmod q &= (\mathbf{r}^T \mathbf{A}^T \mathbf{s} + \mathbf{r}^T \mathbf{e} + m \lfloor q/2 \rfloor) - \mathbf{r}^T \mathbf{A}^T \mathbf{s} \bmod q \\ &= \mathbf{r}^T \mathbf{e} + m \lfloor q/2 \rfloor \bmod q \end{aligned}$$

Public Key Encryption from LWE

$$w - \mathbf{v}^T \cdot \mathbf{s} \bmod q = \mathbf{r}^T \mathbf{e} + m \lfloor q/2 \rfloor \bmod q$$

$$\mathbf{r} \in \{0, 1\}^m$$

\mathbf{e} Gaussian of width σ

$\mathbf{r}^T \mathbf{e}$ is Gaussian of width at most $\sigma\sqrt{m}$

With all but negligible probability, $|\mathbf{r}^T \mathbf{e}| \leq \sigma m$

$$\Rightarrow \mathbf{r}^T \mathbf{e} + m \lfloor q/2 \rfloor \bmod q \approx \begin{cases} 0 & \text{if } m = 0 \\ \pm q/2 & \text{if } m = 1 \end{cases}$$

Lemma: Assuming decisional LWE, encryption scheme is CPA secure

Proof: Let \mathcal{A} be a supposed adversary for the CPA-security of the encryption scheme

Define $W_b(\lambda)$ as the event that \mathcal{A} outputs 1 in the following:

- Run $(\text{sk}, \text{pk}) \leftarrow \text{Gen}(1^\lambda)$, give pk to \mathcal{A}
 - \mathcal{A} produces two msgs m_0, m_1
 - Run $c \leftarrow \text{Enc}(\text{pk}, m_b)$ and give c to \mathcal{A}
 - \mathcal{A} outputs an output guess $b' \in \{0, 1\}$
- Since message is binary, might as well take to be 0,1

Our goal: bound $|\Pr[W_0(\lambda)] - \Pr[W_1(\lambda)]| \leq \epsilon(\lambda)$ for negligible ϵ

Lemma: Assuming decisional LWE, encryption scheme is CPA secure

Proof: Let \mathcal{A} be a supposed adversary for the CPA-security of the encryption scheme

Define $W_b(\lambda)$ as the event that \mathcal{A} outputs 1 in the following:

- Run $(\text{sk}, \text{pk}) \leftarrow \text{Gen}(1^\lambda)$, give pk to \mathcal{A}
- Run $c \leftarrow \text{Enc}(\text{pk}, b)$ and give c to \mathcal{A}
- \mathcal{A} outputs an output guess $b' \in \{0, 1\}$

Our goal: bound $|\Pr[W_0(\lambda)] - \Pr[W_1(\lambda)]| \leq \epsilon(\lambda)$ for negligible ϵ

Lemma: Assuming decisional LWE, encryption scheme is CPA secure

Proof: Let \mathcal{A} be a supposed adversary for the CPA-security of the encryption scheme

Define $W_b(\lambda)$ as the event that \mathcal{A} outputs 1 in the following:

- Give $\text{pk} = (\mathbf{A}, \mathbf{u} = \mathbf{A}^T \cdot \mathbf{s} + \mathbf{e} \bmod q)$ to \mathcal{A}
- Give $(\mathbf{v}^T = \mathbf{r}^T \mathbf{A}^T, w = \mathbf{r}^T \mathbf{u} + b \lfloor q/2 \rfloor \bmod q)$ to \mathcal{A}
- \mathcal{A} outputs an output guess $b' \in \{0, 1\}$

Our goal: bound $|\Pr[W_0(\lambda)] - \Pr[W_1(\lambda)]| \leq \epsilon(\lambda)$ for negligible ϵ

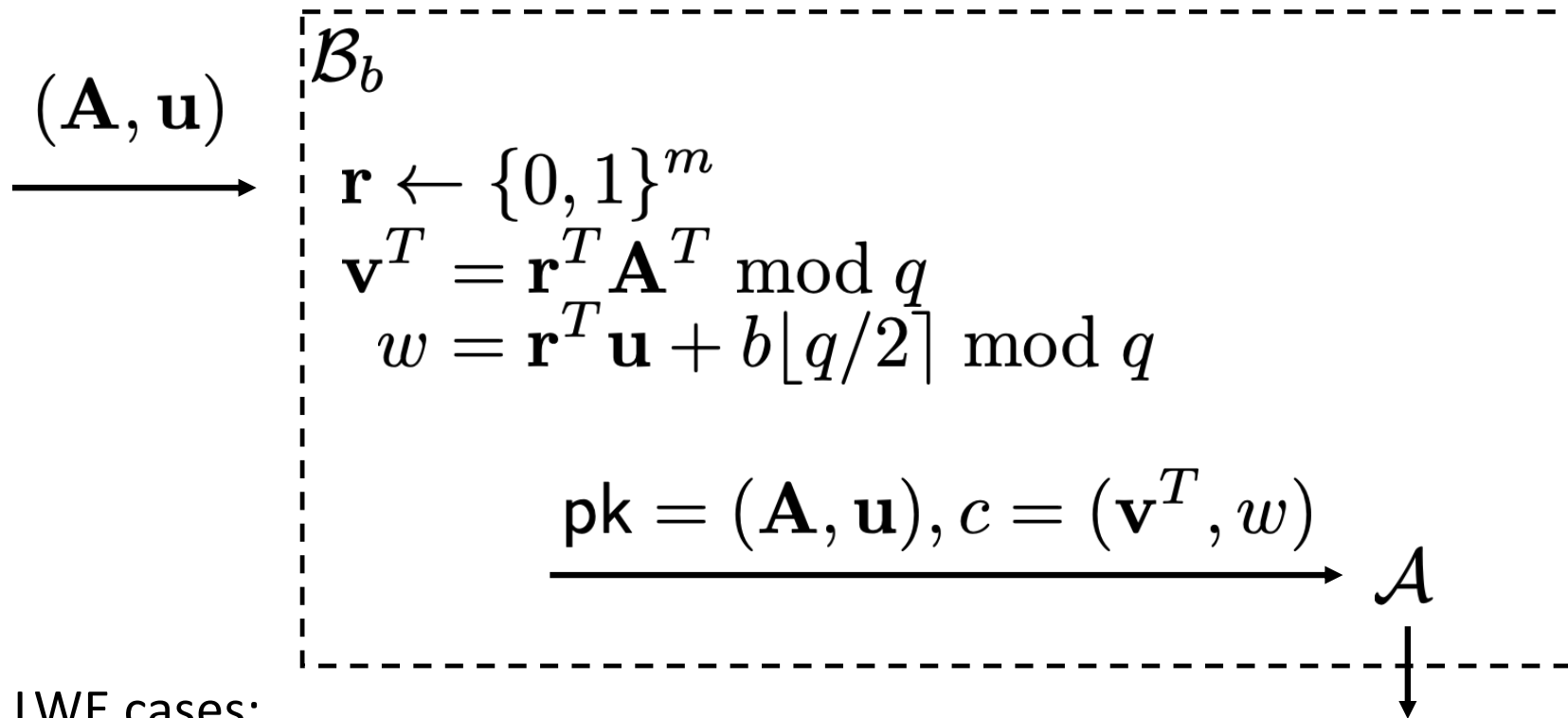
Lemma: Assuming decisional LWE, encryption scheme is CPA secure

Proof:

Define $V_b(\lambda)$ as the event that \mathcal{A} outputs 1 in the following:

- Give $(\mathbf{A}, \mathbf{u} \text{ uniform in } \mathbb{Z}_q^m)$ to \mathcal{A}
- Give $(\mathbf{v}^T = \mathbf{r}^T \mathbf{A}^T, w = \mathbf{r}^T \mathbf{u} + b \lfloor q/2 \rfloor \bmod q)$ to \mathcal{A}
- \mathcal{A} outputs an output guess $b' \in \{0, 1\}$

LWE $\rightarrow |\Pr[W_b(\lambda)] - \Pr[V_b(\lambda)]|$ is negligible



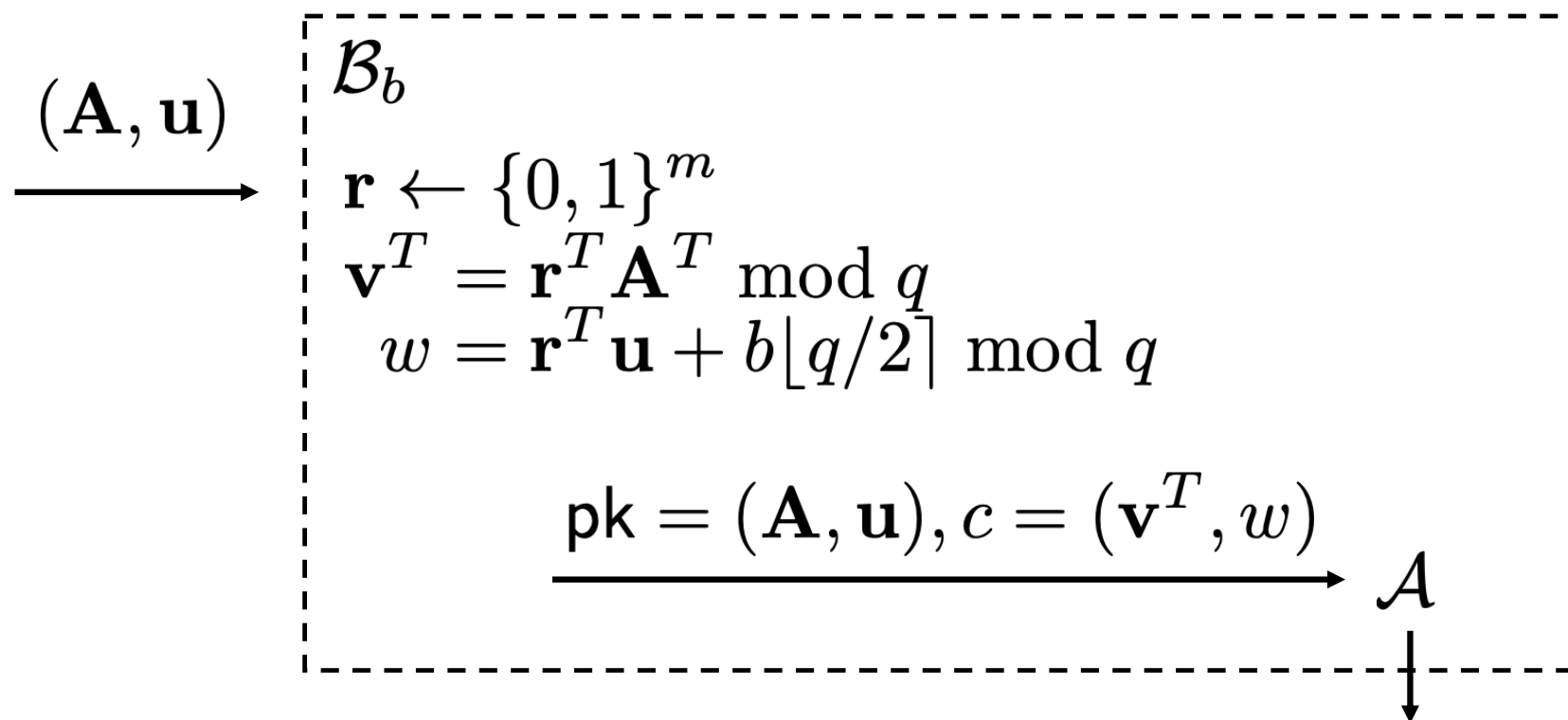
Two LWE cases:

$$\begin{aligned}
 \mathbf{u} &= \mathbf{A}^T \mathbf{s} + \mathbf{e} \bmod q && \Rightarrow \Pr[\mathcal{B}_b(\mathbf{A}, \mathbf{u}) = 1] = \Pr[W_0(\lambda)] \\
 \mathbf{u} &\text{ uniform} && \Rightarrow \Pr[\mathcal{B}_b(\mathbf{A}, \mathbf{u}) = 1] = \Pr[V_0(\lambda)]
 \end{aligned}$$

By LWE, the probability \mathcal{B}_b outputs 1 in the two cases must be negligibly close

Hence $|\Pr[W_b(\lambda)] - \Pr[V_b(\lambda)]|$ is negligible

Notice that \mathcal{B}_b just runs \mathcal{A} once on a single input



This step of the security proof doesn't care about how \mathcal{A} works, just that it does

\mathcal{B}_b 's computation is just \mathcal{A} plus some extra classical computation

Thus $\text{PPT } \mathcal{A} \Rightarrow \text{PPT } \mathcal{B}_b$

$\text{QPT } \mathcal{A} \Rightarrow \text{QPT } \mathcal{B}_b$

Lemma: Assuming decisional LWE, encryption scheme is CPA secure

Proof: claim: $|\Pr[V_0(\lambda)] - \Pr[V_1(\lambda)]|$ is negligible

Recall:

Leftover Hash Lemma: 2-universal hash functions are good randomness extractors

Since entropy of \mathbf{r} is $m \gg (n+1) \log q$

➡ $\mathbf{r}^T \mathbf{A}^T, \mathbf{r}^T \mathbf{u}$ is statistically close to uniform in \mathbb{Z}_q^{n+1}
(even given \mathbf{A}, \mathbf{u})

➡ $(\mathbf{v}^T = \mathbf{r}^T \mathbf{A}^T, w = \mathbf{r}^T \mathbf{u} + b \lfloor q/2 \rfloor \bmod q)$ hides b

This step also doesn't care about how \mathcal{A} works; even unbounded \mathcal{A} are fine

Lemma: Assuming decisional LWE is classically / quantumly secure, encryption scheme is classically / quantumly CPA secure

Actually, all the proofs we've seen so far in this course are like this:

CPA security from LWE

Collision resistance from Dlog on group action

CPA security from DDH on groups / group actions

Hardness of LWE from hardness of SIS

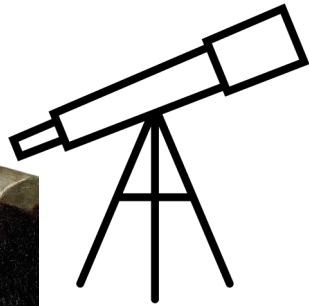
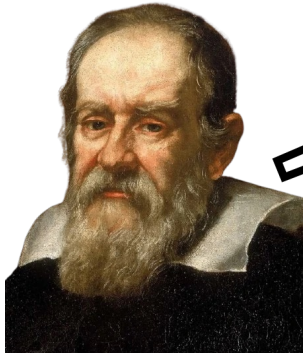
Let's see an example where this fails!

Commitments from collision-resistance

Commitments

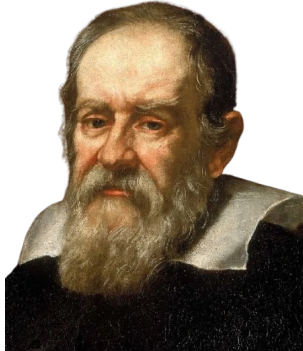


Saturn




Aha! Saturn must
have two moons

Commitments



$c = \text{Com}(\text{"Saturn has two moons!"}) *$



* Actually c was an anagram of the Latin "altissimum planetam tergeminum observavi"
("I have observed the highest planet tri-form")

Galileo sends c as a *commitment* to his “discovery” to establish priority, while also giving himself time to do additional research before actually announcing it

When he announces, everyone checks his announcement against the commitment

Def (Commitment, Syntax): A commitment scheme is an algorithm Com that takes two inputs:

- A message $m \in \{0, 1\}^*$
- Randomness $r \in \{0, 1\}^\lambda$

Once its randomness is fixed, Com is deterministic. It outputs a commitment c

Commit phase: Galileo sends $c \leftarrow \text{Com}(m, r)$ for a random r

Reveal phase: Galileo sends m, r ;
everyone confirms that $c = \text{Com}(m, r)$

Def (Commitment, Statistical Hiding): A commitment scheme is **statistically hiding** if, for all (potentially inefficient) adversaries \mathcal{A} , there exists a negligible function ϵ such that

$$|\Pr[W_0(\lambda)] - \Pr[W_1(\lambda)]| \leq \epsilon(\lambda)$$

where $W_b(\lambda)$ is the event that \mathcal{A} outputs 1 in the following:

- \mathcal{A} produces two msgs $m_0, m_1 \in \{0, 1\}^*$ *of the same length*
- Sample $r \leftarrow \{0, 1\}^\lambda$ and give $c \leftarrow \text{Com}(m, r)$ to \mathcal{A}
- \mathcal{A} outputs an output guess $b' \in \{0, 1\}$

Def (Commitment, Computational Sum-Binding): A commitment scheme is **classically/quantumly sum-binding** if, for all PPT/QPT adversaries \mathcal{A} , there exists a negligible function ϵ such that

$$\Pr[W_0] + \Pr[W_1] \leq 1 + \epsilon(\lambda)$$

where $W_b(\lambda)$ is the event that \mathcal{A} succeeds in the following:

- \mathcal{A} produces a commitment c and two msgs $m_0, m_1 \in \{0, 1\}^*$ *of the same length*
- Give b to \mathcal{A}
- \mathcal{A} tries to output $r \in \{0, 1\}^\lambda$ s.t. $c = \text{Com}(m_b, r)$

Hash functions are good commitments

$$\text{Com}(m, r) = H(m, r)$$

Lemma (informal): With some modifications, if H is sufficiently compressing, then Com is statistically hiding

Proof idea: since H is compressing, it loses information about its input \rightarrow all information about m is lost

Lemma (informal): If H is classically collision-resistant, then Com is classically sum-binding

Intuition: if you could “open” c to two distinct messages, that would give a collision for H

Challenge: in security proof, commitment adversary only gives us one opening. How to we get two for a collision?

Lemma (informal): If H is classically collision-resistant, then Com is classically sum-binding

Proof: Let \mathcal{A} be a supposed adversary contradicting classical sum-binding. Then we have that

$$\Pr[W_0] + \Pr[W_1] \geq 1 + \epsilon(\lambda)$$

for some non-negligible $\epsilon(\lambda)$

Lemma (informal): If H is classically collision-resistant, then Com is classically sum-binding

Proof: $\Pr[W_0] + \Pr[W_1] \geq 1 + \epsilon(\lambda)$

Let $\Pr[W_b|c]$ be the probability conditioned on \mathcal{A} producing a particular commitment c

Call c “good” if $\Pr[W_0|c] + \Pr[W_1|c] \geq 1 + \epsilon(\lambda)/2$

Lemma (informal): If H is classically collision-resistant, then Com is classically sum-binding

Proof:

$$\begin{aligned} 1 + \epsilon(\lambda) &= \Pr[W_0] + \Pr[W_1] \\ &= \sum_{\text{good } c} \Pr[c](\Pr[W_0|c] + \Pr[W_1|c]) + \sum_{\text{bad } c} \Pr[c](\Pr[W_0|c] + \Pr[W_1|c]) \\ &\leq \sum_{\text{good } c} \Pr[c]2 + \sum_{\text{bad } c} \Pr[c](1 + \epsilon(\lambda)/2) \\ &= 2\Pr[\text{good } c] + (1 - \Pr[\text{good } c])(1 + \epsilon(\lambda)/2) \\ &= 1 + \Pr[\text{good } c] + \epsilon(\lambda)/2 - \Pr[\text{good } c]\epsilon(\lambda)/2 \\ &\leq 1 + \Pr[\text{good } c] + \epsilon(\lambda)/2 \end{aligned}$$

Lemma (informal): If H is classically collision-resistant, then Com is classically sum-binding

Proof: $\Pr[\text{good } c] \geq \epsilon(\lambda)/2$

For good c , $\Pr[W_0|c] + \Pr[W_1|c] \geq 1 + \epsilon(\lambda)/2$

➡ $\Pr[W_0|c], \Pr[W_1|c] \geq \epsilon(\lambda)/2$

Lemma (informal): If H is classically collision-resistant, then Com is classically sum-binding

Proof: Now construct the following collision-finder \mathcal{B} :

- \mathcal{B} runs \mathcal{A} until it produces c, m_0, m_1 ; keeps a “program trace” of all internal steps of \mathcal{A}
- \mathcal{B} sends $b = 0$, gets r_0
- \mathcal{B} “rewinds” \mathcal{A} to just after it sends c, m_0, m_1 (using program trace)
- \mathcal{B} sends $b = 1$, gets r_1
- \mathcal{B} outputs $(m_0, r_0), (m_1, r_1)$

Lemma (informal): If H is classically collision-resistant, then Com is classically sum-binding

Proof:

$$\begin{aligned}\Pr[H(m_0, r_0) = H(m_1, r_1) = c] &= \sum_c \Pr[c] (\Pr[W_0|c] \Pr[W_1|c]) \\ &\geq \sum_{\text{good } c} \Pr[c] (\Pr[W_0|c] \Pr[W_1|c]) \\ &\geq (\epsilon(\lambda)/2)^3 = \epsilon(\lambda)^3/8\end{aligned}$$

By the assumption that H is classically collision-resistant, $\epsilon(\lambda)$ must therefore be negligible, a contradiction

Ok, so what happens when we move to quantum?

Recall that \mathcal{B} runs \mathcal{A} , but keeps a program trace so that it can return to a previous state

This simply does not make sense quantumly. By observer effect, extracting r_0 may have irreversibly altered the state of \mathcal{A} , so there's no returning to it

Next time: further exploration of quantum rewinding