

lec 03: coin flipping, commitments, d-log

10 Recap: indistinguishability

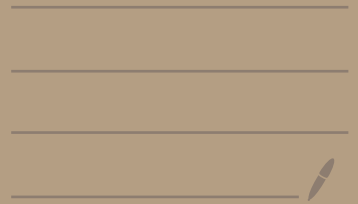
1 Coin flipping

2 Commitments

3 Cyclic groups

4 Pedersen: Commitments from d-log.

5 El Gamal Commitments
from DDH



0 Recap: Indistinguishability

$$D \approx_c D' \text{ if}$$

$$\forall \text{PPT } A, \text{Distadv}[A, D, D'] = \left(\Pr_{d \sim D} [A(d)=1] - \Pr_{d \sim D'} [A(d)=1] \right) \leq \text{negl}(\lambda)$$

$G: S \rightarrow R$ is a PRG if $U(R) \approx_c \{G(s)\}_s$,
we are done with PRGs for the moment,
but we'll use $\approx_c / \approx_s / =$ today.

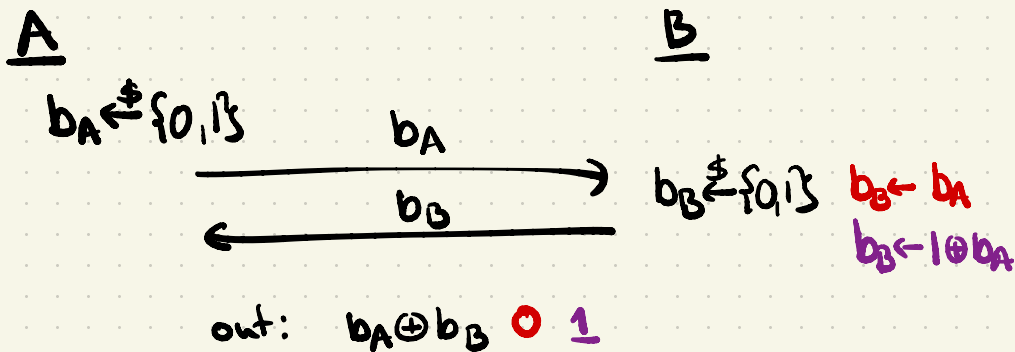
1 Coin Flipping.

[Blum '81 @CRYPTO]

Abstract

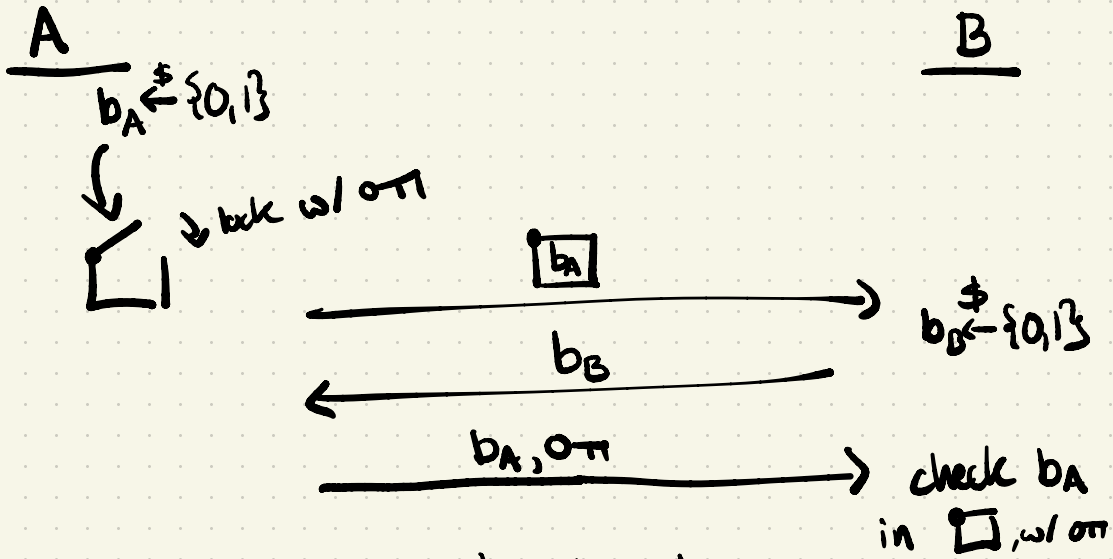
Alice and Bob want to flip a coin by telephone. (They have just divorced, live in different cities, want to decide who gets the car.) Bob would not like to tell Alice HEADS and hear Alice (at the other end of the line) say "Here goes... I'm flipping the coin.... You lost!"

A naive (trusting) protocol:



Problem: B can cheat - and choose the result!

How can we fix the protocol physically?



out: $b_A \oplus b_B$

We need a □ + on, digitally...

Operations:

- sample key
- lock message in box
- check contents w/ key.

• Security

- can't see in box
- can't change contents

2 Commitments

defⁿ $\text{Com}(m, r) \rightarrow c$

↑
message
"b_A"

↑
opening
"key"

↑
commitment
"locked box"

New protocol, using $\text{Com}: \{0,1\} \times R \rightarrow C$

A

$$b_A \xleftarrow{\$} \{0,1\}$$

$$r \xleftarrow{\$} R$$

$$c \leftarrow \text{Com}(b_A, r)$$

← put b_A in box

B

← can't see b_A

$$\xrightarrow{c}$$

$$b_B \xleftarrow{\$} \{0,1\}$$

$$\xleftarrow{b_B}$$

$$\xrightarrow{b_A, r}$$

check

b_A can't change.

$$c \stackrel{?}{=} \text{Com}(b_A, r)$$

$$\text{out: } b_A \oplus b_B$$

Commitment Security properties

Hiding: "c hides m"

$$\forall m, m', \quad \{\text{Com}(m, r)\}_r \approx_c \{\text{Com}(m', r)\}_r$$

this is computational.

Binding: "c = Com(m, r) can't be opened to m'"

$$\forall \text{PPT } A, \quad \Pr_A[A(\cdot) \rightarrow (m, m', r, r): m \neq m' \wedge \text{Com}(m, r) = \text{Com}(m', r)]$$

$$\leq \text{negl}$$

Note: we wrote computational hiding. Other options:

perfect hiding uses =

statistical hiding uses $\approx$,

So now, we need a commitment scheme...

[3] Cyclic groups

First, we'll need a math object, the cyclic group.

"Let G be a group of order p, generated by g"

G is a set, with a binary ($\cdot$) operation

$$(\cdot) : G \times G \rightarrow G$$

$\uparrow$ commutative, associative, etc.

($\cdot$) in G works just like ($\cdot$) in $\mathbb{R}$ (the reals)

• it is commutative & associative

• There is an identity $1 \in G$ s.t. $\forall h \in G, h \cdot 1 = 1 = 1 \cdot h$

• Exponentiation h^n is repeated ($\cdot$): $\underbrace{h \cdot h \cdot \dots \cdot h}_n$

• it's efficient: h^n takes $O(\log n)$ ($\cdot$)'s

• There are also inverses + division: $h \mapsto 1/h$

• it's also efficient

• You can define logarithms: $x = \log_g h$ if $g^x = h$.

• these are often inefficient—see later...

• But, unlike $\mathbb{R}$, G is a finite set!

• $|G| = p$ ← "order" is set size

• "g generates G" means

G (the set) = $\{1, g, g^2, g^3, \dots, g^{p-1} = 1\}$ are in $\mathbb{Z}_p$

these are all the things in G ! (mod p)

there are no others.

• Since $g^p = g^0 = 1$, we only care about exponents (mod p).

• So, we regard exponents as $\mathbb{Z}_p$

• integers modulo p

• recall: in $\mathbb{Z}_p$, " a/b " is the value $\in \mathbb{Z}_p$ s.t.
 $(a/b) \cdot b = a \pmod{p}$

4) Pedersen Commitments!

Take $h \in G \setminus \{1\} \leftarrow$ a public parameter

$\text{Com}(m \in \mathbb{Z}_p, r \in \mathbb{Z}_p) \rightarrow c \in G:$

$$c \leftarrow g^m h^r$$

Security (Hiding):

Pedersen has perfect hiding.

pf. fix m, m'

goal: $\{g^m h^r\}_r = \{g^{m'} h^r\}_r$ this is the

we'll show $\rightarrow \textcircled{11} \textcircled{11} \leftarrow$ same thing $U(G)$

Since r is uniform in $\mathbb{Z}_p$,
 h^r is uniform in G .

Since h^r is also independent of g^m ,
 $g^m h^r$ is uniform in G .

Another pf:

$$\begin{aligned} \Pr_r [g^m h^r = g'] &= \Pr_r [h^r = g'/g^m] \\ &= \Pr_r [r = \log_h (g'/g^m)] \end{aligned}$$

$\forall h, h' \in G, h \neq 1,$

$\log_h h'$ is the unique x s.t. $h^x = h'$

logarithms are defined, but may be hard to compute some constant $\in \mathbb{Z}_p$

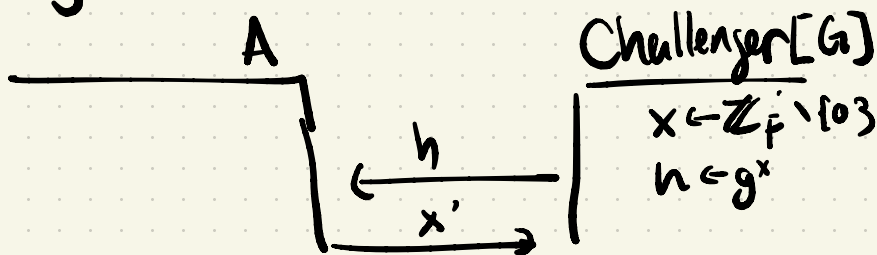
$$= 1/p$$

So, $g^r h^r$ is uniform.

Security (Binding):

We'll assume that the discrete logarithm problem "d-log" is hard in G :

D-Log $[G]$:



A 's advantage: $\Pr[x' = x]$

Another phrasing:

$\forall$ PPT A ,

probability must be negl

$$\Pr_{x \in \mathbb{Z}_p^* \setminus \{0\}} [A(g^x) = x] \leq \text{negl}$$

Now, proving d-log $\Rightarrow$ Pedersen binding.

Fix a binding adversary $A(g, h) \rightarrow (m, m', r, r')$,
 $\uparrow$ public parameters

with advantage $\neq \text{negl.}$

- How will we define B to break $d\text{-log}$?
- Well, when A wins:

$$\underline{g^m h^r} = \underline{g^{m'} h^{r'}}$$

- So A knows 2 representations of one group element.

- Rule: 2 representations usually means you can break $d\text{-log}$.

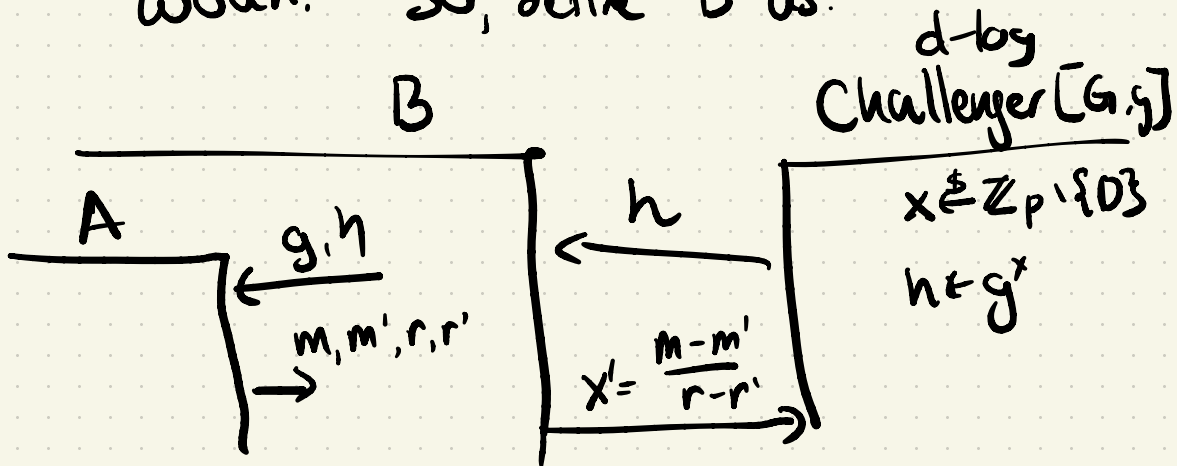
$$g^m h^r = g^{m'} h^{r'} \quad \begin{matrix} (\cdot) g^{m'} (\cdot) / h^r \\ (\cdot)^{\frac{1}{r-r'}} \end{matrix}$$

$$g^{m-m'} = h^{r'-r}$$

$$g^{\left(\frac{m-m'}{r-r'}\right)} = h$$

$$\frac{m-m'}{r-r'} = \log_g h$$

woah! so, define B as:



And x will always equal x' , but the argument above, so long as $r \neq r'$, so that $r-r'$ is invertible

need : $r \neq r'$

pf: towards $\Rightarrow \Leftarrow$, assume $r = r'$

$$\Rightarrow h^r = h^{r'}$$

$$\Rightarrow g^m h^r = g^{m'} h^{r'}$$

$$\Rightarrow g^m = g^{m'}$$

$$\Rightarrow m = m'$$

$\Rightarrow \Leftarrow$

We've show that B's d-log advantage equals A's binding advantage, which is not negl.



5 (Bonus): El Gamal commitments

Pedersen commitments are perfectly hiding and computationally binding.

We'll now do a new commitment scheme (El Gamal) which is computationally hiding and perfectly binding.

The scheme is this:

$$\text{EG.Com}(m \in \mathbb{Z}_p, r \in \mathbb{Z}_p) \rightarrow c \in G^2$$

$$c_0 \leftarrow g^m h^r$$

$$c_1 \leftarrow g^r$$

Perfect Binding:

It suffices to show that if

$m \neq m'$, then there are no r, r' such that

$$\text{EG.Com}(m, r) = \text{EG.Com}(m', r')$$

pf. suppose $\uparrow$, towards $\Rightarrow$

$$\text{then, } g^m h^r = g^{m'} h^{r'} \quad \text{and} \quad g^r = g^{r'}$$

$$\text{by the 2}^{\text{nd}}, \quad r = r'$$

$$\text{so, } g^m h^r = g^{m'} h^r$$

$$\text{so, } g^m = g^{m'}$$

so $m = m'$
which contradicts $m \neq m'$.

Computational hiding

Goal:

Fix m, m', PPTA .

We'll show that for A ,

$$\{EG.Com(m, r)\}_r \approx_c \{EG.Com(m', r)\}_r$$

By showing

$$\approx_c U(G^2) \approx_c$$

m and m'

(the same pf works for both, since m/m' are arbitrary, so we proceed w/ m).

We'll do a reduction from a new assumption,

Decisional Diffie Hellman (DDH):

$$DDH[G] \triangleq \{(g^\alpha, g^\beta, g^\gamma)\}_{\alpha, \beta, \gamma} \approx_c \{(g^\alpha, g^\beta, g^{\alpha\beta})\}$$

Reduction:

Assume A w/ $\text{Distadv}[A, \{Com(m, r)\}_r, U(G^2)] \neq \text{negl}$.

Define B for DDH:

gets $g^\alpha, g^\beta, g^\gamma$ (maybe $\gamma = \alpha\beta$, maybe not)

Gives $h = g^{\alpha}$, $c_1 = g^{\beta}$, $c_0 = g^{\gamma} g^{\eta}$ to A ,
and copies A 's output

$$\text{Distadv}[B, \{(g^{\alpha}, g^{\beta}, g^{\alpha\beta})\}_{\alpha, \beta}, \{(g^{\alpha}, g^{\beta}, g^{\gamma})\}_{\alpha, \beta, \gamma}]$$

$$= \left| \Pr[A(h = g^{\alpha}, c_0 = g^{\alpha\beta} g^{\eta}, c_1 = g^{\beta}) = 1] \right.$$

$$\left. - \Pr[A(h = g^{\alpha}, c_0 = g^{\gamma\eta}, c_1 = g^{\beta}) = 1] \right|$$

since α, β, γ are uniform and
independent, this is stat. close to

$$\Pr_{\substack{g', g'' \in G \\ h \in G \setminus \{1\}}} [A(h, g', g'') = 1]$$

The right side of

$$\text{Distadv}[A, \{\text{com}(m, r)\}_r, u(g^{\eta})]$$

(with h too)

great! now let's work
on the left

$$\Pr[A(h = g^{\alpha}, c_0 = g^{\alpha\beta} g^{\eta}, c_1 = g^{\beta}) = 1]$$

$$\Pr[A(h, c_0 = h^{\beta} g^{\eta}, c_1 = \beta^{\beta}) = 1]$$

$$\Pr[A(h, \text{com}(m, \beta)) = 1]$$

the left side of

So:

$$= \text{Distadv}[A, \{\text{Com}(m, \beta)\}, \mathcal{U}(G^*)]$$

$\neq \text{negl.}$

