LECTURE 13 23/11

NUMBER THEORY

Last Time

$(\mathbb{Z}_p^* = G, g, p)$

Alice		Bob
$x \leftarrow \$ \mathbb{Z}_{p-1}$		$y \leftarrow \$ \mathbb{Z}_{p-1}$
	$\xrightarrow{g^x}$	
	$\xleftarrow{g^y}$	
$K = g^{xy}$		$K = g^{xy}$

(Passive Eve)

$\mathbb{Z}_p^*$ is a cyclic group with generator g:

$GAME^{DL}_{A}(\lambda)$

$A(1^\lambda)$		$\mathcal{C}(1^\lambda)$
		$(G, g, p) \leftarrow \$ \text{GroupGen}(1^\lambda)$
		$x \leftarrow \$ \mathbb{Z}_{p-1}$
	$\xleftarrow{(G, g, p, g^x)}$	
	$\xrightarrow{x'}$	
		OUTPUT

1 iff $x' = x$

$GAME_{\mathcal{A}}^{CDH}(\lambda)$

$\mathcal{A}(1^\lambda)$ | $\mathcal{C}(1^\lambda)$

$\mathcal{C}$: $params = (\mathbb{G}, g, p)$

$\mathcal{C}$: $x, y \leftarrow \$ \ \mathbb{Z}_{p-1}$

$\mathcal{C} \to \mathcal{A}$: $(params, g^x, g^y)$

$\mathcal{A} \to \mathcal{C}$: K

OUTPUT 1 iff $K = g^{xy} \bmod p$

$GAME_{\mathcal{A}}^{DDH}(\lambda, b)$

$\mathcal{A}(1^\lambda)$ | $\mathcal{C}(1^\lambda)$

$\mathcal{C}$: $params = (\mathbb{G}, g, p)$

$\mathcal{C}$: $x, y \leftarrow \$ \ \mathbb{Z}_{p-1}$

$\mathcal{C}$: $K = \begin{cases} g^{xy} \bmod p & (b=0) \\ g^z, \ z \leftarrow \$ \ \mathbb{Z}_{p-1} & (b=1) \end{cases}$

$\Updownarrow$

$K \leftarrow \$ \ \mathbb{G}$

$\mathcal{C} \to \mathcal{A}$: $(params, g^x, g^y, K)$

$\mathcal{A} \to \mathcal{C}$: b'

DEF: DDH holds w.r.t. GroupGen if $\forall$ PPT $\mathcal{A}$:

$$GAME_{\mathcal{A}}^{DDH}(\lambda, 0) \approx_c GAME_{\mathcal{A}}^{DDH}(\lambda, 1)$$

Note: DDH $\Rightarrow$ CDH $\Rightarrow$ DL

Q: Does CDH $\Rightarrow$ DDH?

A: Not in general. In particular, CDH believed to hold in $\mathbb{G} = \mathbb{Z}_p^*$ but DDH does not hold.

Consider the group of QUADRATIC RESIDUES

$$QR_p = \{y : y = x^2 \mod p\}$$
$$= \{y : y = x^z \mod p\} \quad \text{with even } z$$

g^z

We can test efficiently if $y \leftarrow \$ \, QR_p$. We check $y^{(p-1)/2} \mod p = 1$. Why? Because if $y = g^{2z'}$ then $y^{(p-1)/2} = (g^{2z'})^{(p-1)/2} = g^{(p-1)z'} = 1 \mod p$. Otherwise, $y = g^{2z'+1}$ then $y^{(p-1)/2} = (g^{(2z'+1)})^{(p-1)/2} = g^{(p-1)/2} \neq 1 \mod p$

Given g^{xy}, it's easy to see that

$g^{xy} \in QR_p$ iff either $g^x \in QR_p$

or $g^y \in QR_p$

$\Rightarrow$ Over the choice of x, y, z

$g^{xy} \in QR_p$ w.p. $\frac{3}{4}$

$g^z \in QR_p$ w.p. $\frac{1}{2}$

$\Rightarrow$ $\exists$ PPT $\mathcal{A}$ breaking DDH in $\mathbb{G} = \mathbb{Z}_p^*$

g^x, g^y, g^{xy} = DDH TUPLE

g^x, g^y, g^z = NON-DDH TUPLE

How to fix it? Take $G = QR_p$ with $p = 2q+1$, p and q primes. Then G is cyclic with order $q = \frac{p-1}{2}$

$\Longrightarrow$ DDH believed to hold

$\rightsquigarrow$ OWF $\not\Rightarrow$ Passively Secure KE

MINICRYPT | CRYPTOMANIA

SKE PRP OWF PRF PRG

PKE KE ($\Leftarrow$ DDH) CHR

DDH $\Rightarrow$ DL $\Rightarrow$ OWPs $(y = g^x \bmod p = f(x))$

Let's be more efficient!

$\boxed{*}$ PRGs. $(G, g, q) \leftarrow \$ \text{GroupGen}(1^\lambda)$

$x, y \leftarrow \$ \mathbb{Z}_q$

$G_{g,q}(x,y) = (g^x, g^y, g^{xy})$ DDH TUPLE

$G_{g,q} : \mathbb{Z}_q^2 \rightarrow G^3$

Note: easy to improve the stretch.

$$G_{g,q} : \mathbb{Z}_q^{t+1} \rightarrow G^{2t+1}$$

$$G_{g,q}(x, y_1, \dots, y_t) = (g^x, g^{y_1}, g^{xy_1}, \dots, g^{y_t}, g^{xy_t})$$

THM: The above is a PRG iff DDH holds $\forall\, t(\lambda) = \text{poly}(\lambda)$

PROOF: Follows by hybrid argument, but the reduction is NOT TIGHT. We now give a TIGHT reduction.

Assume $\exists$ PPT $\mathcal{A}$ that breaks above PRG w.p. $\frac{1}{poly(\lambda)}$.

This means $\mathcal{A}$ can tell apart:

$$(g^{x}, g^{y_1}, g^{xy_1}, \ldots, g^{y_t}, g^{xy_t})$$

$$(g^{x}, g^{y_1}, g^{z_1}, \ldots, g^{y_t}, g^{z_t})$$

$x, y_1, z_1, \ldots, y_t, z_t \leftarrow \$ \, \mathbb{Z}_q$

TIGHT reduction: $\exists$ $\mathcal{A}_{DDH}$ breaking DDH with some probabilit

$\mathcal{A}(1^\lambda)$		$\mathcal{A}_{DDH}(1^\lambda)$		$\mathcal{C}_{DDH}(1^\lambda)$
		$u_j, v_j \leftarrow \$ \, \mathbb{Z}_q$		$params = (\mathbb{G}, g, q)$
				$x, y \leftarrow \$ \, \mathbb{Z}_q$
			$\xleftarrow{params,\, g^x,\, g^y,\, g^z}$	z: $xy \bmod q$ or $\leftarrow \$ \, \mathbb{Z}_q$
		$g^{y_j} = (g^y)^{u_j} \cdot g^{v_j}$		
		$g^{z_j} = (g^z)^{u_j} \cdot (g^x)^{v_j}$		
	$\xleftarrow{params,\, g^x,\, g^{y_1},\, g^{z_1},\, \ldots,\, g^{y_t},\, g^{z_t}}$			
	$\xrightarrow{b'}$			
			$\xrightarrow{b'}$	

Analysis: Let $z = xy + \beta$ where $\beta = 0$ (if DDH) or $\beta \leftarrow \$ \, \mathbb{Z}_q$ (if NOT DDH)

Let's look at the exponents:

$$y_j = y u_j + v_j \qquad z_j = z u_j + x v_j =$$
$$= (xy + \beta) u_j + x v_j =$$
$$= \beta u_j + x (y u_j + v_j) =$$
$$= \beta u_j + x y_j$$

First, since v_j is UNIFORM, so is y_j.

Second, if $\beta = 0$, $z_j = x y_j$ which gives the BLACK DISTRIBUTION of the PRG.

Third, if $\beta \leftarrow \$ \mathbb{Z}_q$, the z_j are all random and independent (since u_j's are random and independent of the y_j's)

So, the reduction random simulates the RED DISTRIBUTION of the PRG.

A distingue con probabilità con 1 su poly che è la stessa probabilità che ha l'attaccante di rompere il DDH ∎

$\boxed{*}$ PRFs. NAOR-REINGOLD params $\leftarrow \$$ GroupGen(1^λ)

$$\mathcal{F}_{NR} : \left\{ F_{q,g,\vec{a}} : \{0,1\}^n \rightarrow \mathbb{G} \right\}_{\vec{a} \in \mathbb{Z}_q^{n+1}}$$

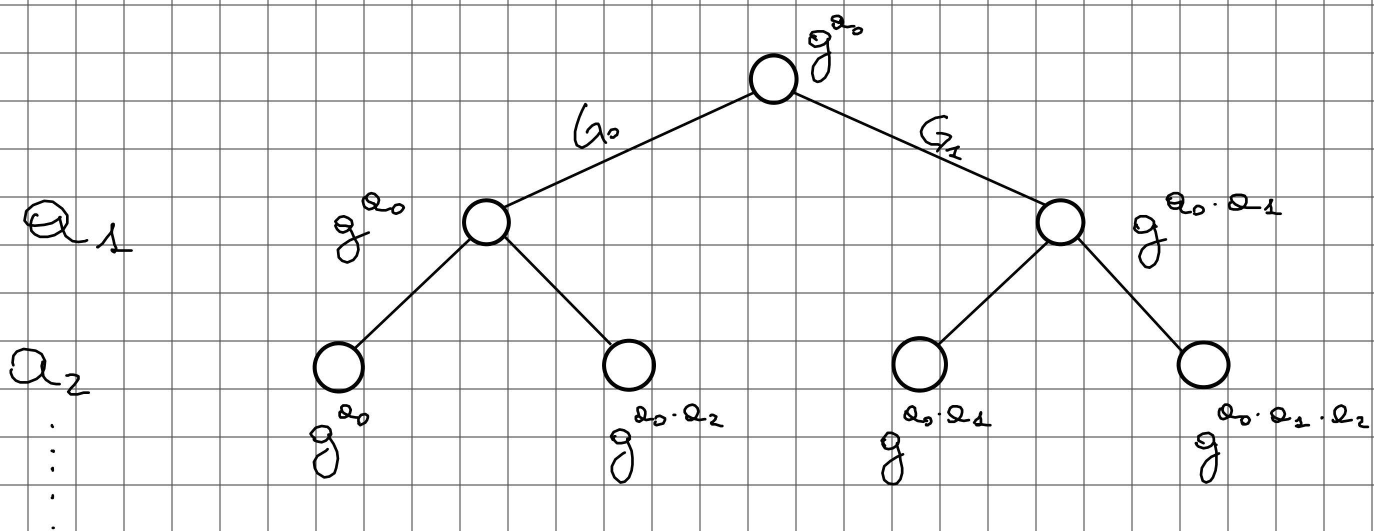
where $F_{q,g,\vec{a}}(\underset{\{0,1\}}{\underset{\cap}{x_1}}, \dots, \underset{\{0,1\}}{\underset{\cap}{x_n}}) = (g^{a_0})^{\prod_{i=1}^{n} a_i}$, with $\vec{a} = (a_0, a_1, \dots, a_n)$

Note: complexity is at most n multiplications to determine exponent $a_0 \cdot \prod_{i=1}^{n} a_i^{x_i}$ + $2n$ multiplications for modular exponentions (SQUARE AND MULTIPLY)

$\Rightarrow$ SECURE under DDH.

The PROOF is a special case of GGM with PRG

$$G^{q,g,a}(g^b) = G_0(g^b) \,\|\, G_1(g^b) = (g^b, g^{ab})$$



$\boxed{*}$ CRH. $\mathcal{H} = \{ H_{g_1, g_2, p, q} : \mathbb{Z}_q^2 \to \mathbb{QR}_p \}$

$\mathbb{G} = \mathbb{QR}_p$; $p = 2q+1$; p and q PRIMES

g_1 is a generator ; $g_2 \leftarrow \$ \, \mathbb{G}$

where $H(x_1, x_2) = g_1^{x_1} \cdot g_2^{x_2} \mod p$ $\approx 2\lambda \to \lambda$ COMPRESSION

Note: SECURE under DL!

Assume $\exists$ PPT $\mathcal{A}$ finding collisions (w.p. $\frac{1}{poly}$)

$(x_1, x_2) \neq (x_1', x_2')$ s.t. $g_1^{x_1} \cdot g_2^{x_2} = g_1^{x_1'} \cdot g_2^{x_2'} \mod p$

$\Rightarrow$ $g_1^{x_1 - x_1'} = g_2^{x_2' - x_2} \mod p$

$\Rightarrow$ $g_2 = g_1^{(x_1 - x_1') \cdot (x_2' - x_2)^{-1}}$ (inverse exist in $\mathbb{Z}_q$ as q PRIME)

$\Rightarrow (x_1 - x_1') \cdot (x_2' - x_2)^{-1}$ is the DL of g_2

PUBLIC-KEY ENCRYPTION

pK (PUBLIC)

Alice: pK

$c \leftarrow \$ \, Enc(pK, m)$

$\xrightarrow{\quad c \quad}$

Bob: pK, sK

$m = Dec(sK, c)$

$\Pi = (KGen, Enc, Dec)$

$(pK, sK) \leftarrow \$ \, KGen(1^\lambda)$

PROBLEM: Need to certify pK's (Eve may replace Bob's pK with his)

SOLUTION: PKI. For now: Ignore it, just assume there's a way to do it

$GAME^{cpa}_{\Pi,A}(\lambda, b)$

$A(1^\lambda)$ | **$C(1^\lambda)$**

C: $(pK, sK) \leftarrow \$ \, KGen(1^\lambda)$

$A \xleftarrow{\quad pK \quad} C$

(Now Alice can encrypt any $m \in \mathcal{M}$ under pK on her own)

$A \xrightarrow{\quad m_0^*, m_1^* \in \mathcal{M} \quad} C$

C: $c^* \leftarrow \$ \, Enc(pK, m_b)$

$A \xleftarrow{\quad c^* \quad} C$

$A \xrightarrow{\quad b' \quad} C$

$\mathrm{GAME}^{cca}_{\Pi,\mathcal{A}}(\lambda, b)$