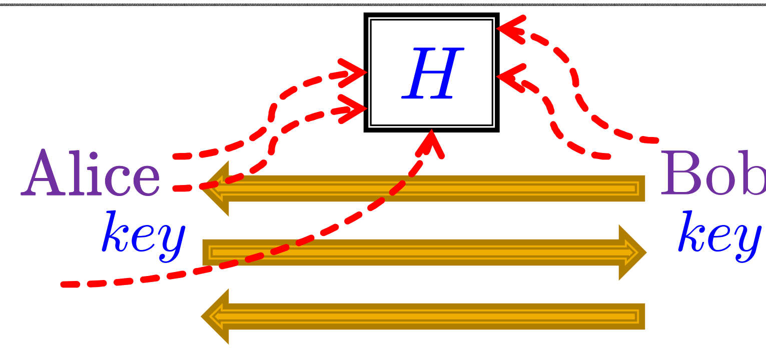
Princeton University

Mohammad Mahmoody-Ghidary
Joint work with **Boaz Barak**

Merkle Puzzles are Optimal.

Spoiler:
Key Exchange, Random Oracle, The Result

Key Exchange:



Security: For every eavesdropping Eve outputting k_{EVE} : $\Pr[\, k_{EVE} = \text{key}] \approx 0$

Random oracle model: All parties have *black-box* access to a random function H:$\{0,1\}^n \rightarrow \{0,1\}^n$

Our Result: $\forall$ n-query protocol, $\exists$ $O(n^2)$-query Eve:

$\Pr[\, k_{EVE} = \text{key}] \approx 1$

Merkle '74: $\exists$ n-query protocol (using some puzzles!),

$\forall$ $o(n^2)$-query Eve: $\Pr[\, k_{EVE} = \text{key}] \approx 0$

Rest of the Talk

- Part I: Some History and Merkle's Protocol
- Part II: Our Attack's Description & Analysis

History I – Modern Crypto

- 1974: Merkle's Key-Exch scheme w/ $\Omega(n^2)$ security (using his puzzles)
  Could be formalized in Random Oracle Model
- 1976: Diffie-Hellman's Key-Exch scheme (related to discrete log)
- 1978: Rivest-Shamir-Addleman (related to factoring).
- 1779: Rabin (exactly based on Factoring!)
- During 80': What are the *minimal* assumptions?...

History II – Postmodern Crypto

- 80'--: One-way function effect.
  ⇒ : Priv-Key, Dig-Sign, ZK, PRG, PRF, PRP Commitments,…
- 1989: Impagliazzo-Rudich No "black-box way" to get Key-Exch from OWF
  [Sim98, GKMRV00, GMR01, Fis02, HR04, HH09, KST99, GT00, GGK03, HK05, LTW05, HHRS07,BMG07, BMG08, …..]
- The Main Step in [IR89]:
  Break *any* Key-Exch in Random Oracle Model w/ $O(n^6)$ queries

What left to do?

Left Open in [IR89] :

1) Get weak-Key-Exch from OWF? ✓ [BIG08]

2) Can we get $\Omega(n^6)$ security from RO? ×

Main Thm: $\forall$ Key-Exch protocol w/ n queries to RO,
$\exists$ **ADV** asking $O(n^2)$ queries, $\Pr[\text{ADV finds key}] \approx 1$

Cor : Merkle's scheme ['74] is optimal in OR model.
Also [BIG08] is optimal (using exp-hard OWF).

Merkle's Protocol

Alice	Bob
Pick $k_1,...k_n$ at rand	
Put k_i in puzzle P_i	Take the puzzles
Sent $P_1,...P_n$ to Bob	from Alice
	Solve a random P_j to get k_j

Main Thm: $\forall$ n-query protocol, $\exists$ $O(n^2)$-query Eve s.t.

$\Pr[\ k_{EVE} = \text{key}] \approx 1$

Puzzles : Solving a fixed P_i takes time n^2
Solving a random P_j takes time n

w/ Random Oracle H: $P_j = H(k_j)$
Choose k_i from S where $|S| = n^2$

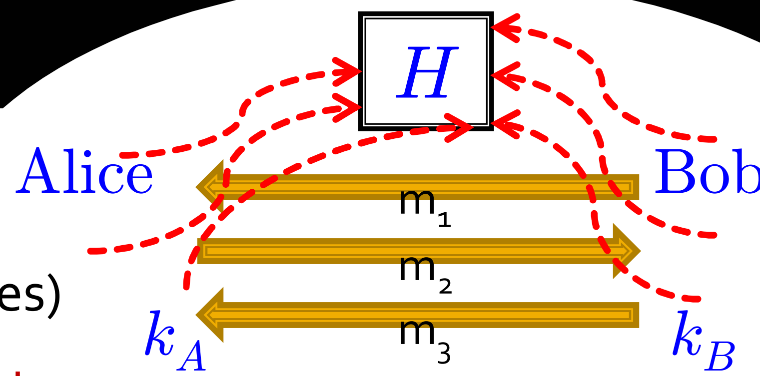
In fact: The Latter is Merkle's original scheme (not published) and the puzzles above are only "similar" to his actual puzzle scheme published in '78....

Rest of the Talk

- Part I: Some History and Merkle's Protocol

- Part II: Our Attack's Description & Analysis

Intro to Attack



- A: Alice's view : (Bob's view B is similar)

  rand_A + $\{m_1, m_2 \ldots\}$ + Q_A (her oracle queries)

- output same keys $\Rightarrow$ A and B are correlated.
- Eve's view E : rand_E + $\{m_1, m_2 \ldots\}$ + Q_E (her oracle queries)
- Hope: E contains all the cor between A and B : $(A|E)$, $(B|E)$ $\approx$ indep

  then if Eve samples A' conditioned on $E \Rightarrow \Pr[k_A' = k_B] = \Pr[k_A = k_B]$

- One Idea : Ask the whole oracle H ! (bad: 2^n queries)

- Our Attack: (1) : If (*) $Q_A \cap Q_B \subset Q_E$ hold $\Rightarrow$ make $(A|E)$, $(B|E)$ $\approx$ indep

  (2) : make (*) $Q_A \cap Q_B \subset Q_E$ *always hold* by only $O(n^2)$ queries.

- [IR89]: (1) if (*) $\Rightarrow$ "$\mathrm{Cor}(A \mid E \; , \; B \mid E) = 0$" or "a pot.func" increases.

  (2) make (*) hold with $O(n^6)$ queries.

The Attack.

A : Alice's view so far
B : Bob's view so far
Q_A, Q_B, Q_E: their oracle queries.

Attack's Algorithm:

Assume that (*) $Q_A \cap Q_B \subset Q_E$ so far.

Conditioned on Eve's info -- and(*):

If $\exists$ q s.t. $\Pr[q \in Q_A \cup Q_B] \geq 1 / (1000n) \Rightarrow$ Eve asks q

We "will see":

(cond on E): $\text{dist } A$ and $\text{dist } B$ become "almost" indep .

$\Rightarrow$ Eve can find key.

We won't see but true!:

$|Q_E| \leq O(n^2)$ (Attack is efficient)

Alice & Bob's distributions as a Graph

A : Alice's view so far
B : Bob's view so far
Q_A, Q_B, Q_E: their oracle queries.

Attack's Algorithm:

Assume that (*) $Q_A \cap Q_B \subset Q_E$ so far.
Conditioned on Eve's info -- and(*):
If $\exists$ q s.t. $\Pr[q \in Q_A \cup Q_B] \geq 1/(1000n) \Rightarrow$ Eve asks q

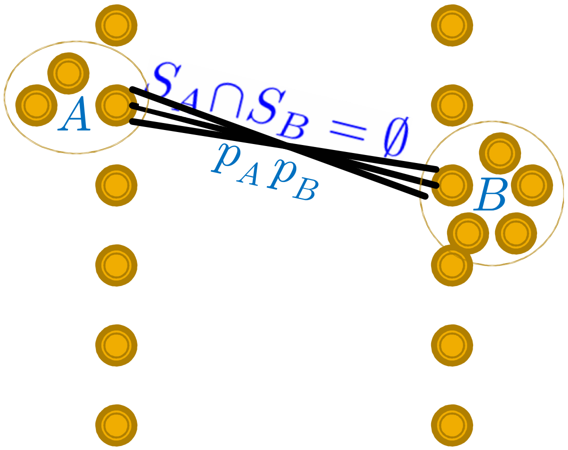
- Let S_A be queries asked by A and *not* by Eve

  S_B be queries asked by B and *not* by Eve

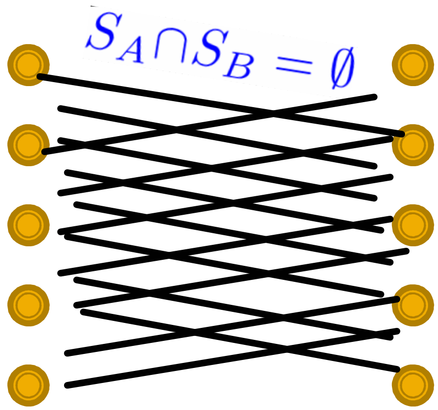
Note : If $S_A \cap S_B \neq \emptyset \Rightarrow \Pr[(A,B)] = 0$

Claim: If $S_A \cap S_B = 0 \Rightarrow \Pr[(A,B)] = p_A \cdot p_B$

Now: $\mathrm{dist}\,(A,B)$ is choosing random edge $(A \sim B)$!



Pure Combinatorics!



Lemma:

$A \sim B$ iff $S_A \cap S_B = \emptyset$ for $|S_A|, |S_B| \leq n$ and

$\forall q, \quad \Pr_{(A,B)\in E(G)}[q \in S_A \cup S_B] \leq 1/(1000n)$

Then every vertex in G is connected to at least 99% of the other side.

Corollary:

sampling a random edge $A \sim B$ is almost same as choosing A and B independently.

Open Questions

- $O(n^2)$ bound for random permutations
  (we improve [IR89]'s $O(n^{12})$ bound to $O(n^4)$)

  can also consider ideal cipher, other "symmetric" primitives.

- Rule out a "classical" const with non-trivial (i.e., $\omega(n)$) security w.r.t. *quantum* attacks? [BrassardSalvail08, BihamIshaiGoren08]

- Find non-black-box constructions of key exchange from one-way functions.

Thank You!