Updates to Definition 2 and Theorem 5

Sarang Noether

July 2, 2020

Let $\mathbb{G}$ be a finite cyclic group over $\mathbb{F}_p$, where $p > 2$ is prime. Let G be a fixed generator of $\mathbb{G}$. Let $n, d > 1$ be fixed integers. Let $\mathcal{H}^p$ be a random oracle with codomain $\mathbb{G}$. Let $\mathcal{H}_0^s$ and $\{\mathcal{H}_j^s\}_{j=1}^{d-1}$ be random oracles with codomain $\mathbb{F}_p$.

Definition (Random Oracle Decisional Diffie-Hellman (RO-DDH))**.** We say any PPT algorithm $\mathtt{A}$ that can succeed at the following game in time at most t with advantage least $\epsilon > 0$ over random chance is a (t, ϵ, q)-solver of the random oracle decisional Diffie-Hellman game.

- The challenger chooses a bit $b \in \{0, 1\}$ uniformly at random.
- If $b = 0$, then the challenger chooses $\{r_i\}_{i=0}^{q-1}$ from $\mathbb{F}_p$ uniformly at random, sets

  $$S := \{(R_i, R_i', R_i'')\}_{i=0}^{q-1} = \{(r_i G, \mathcal{H}^p(r_i G), r_i \mathcal{H}^p(r_i G))\}_{i=0}^{q-1},$$

  and sends S to $\mathtt{A}$.
- If instead $b = 1$, then the challenger chooses $\{(r_i, r_i'')\}_{i=0}^{q-1}$ from $\mathbb{F}_p^2$ uniformly at random, sets

  $$S := \{(R_i, R_i', R_i'')\}_{i=0}^{q-1} = \{(r_i G, \mathcal{H}^p(r_i G), r_i'' G)\}_{i=0}^{q-1},$$

  and sends S to $\mathtt{A}$.
- $\mathtt{A}$ is granted access to the random oracle $\mathcal{H}^p$.
- $\mathtt{A}$ returns a bit $b' \in \{0, 1\}$; we say $\mathtt{A}$ succeeds if and only if $b' = b$.

We say that random oracle Diffie-Hellman group elements are hard to distinguish from random in $\mathbb{G}$ if any (t, ϵ, q)-solver of this game has negligible advantage ϵ.

Remark. We assume that if the classic decisional Diffie-Hellman (DDH) game is hard in $\mathbb{G}$, then so is the RO-DDH game. Indeed, note that DDH asks an adversary to distinguish between distributions of tuples of the form $(rG, r'G, rr'G)$ and $(rG, r'G, r''G)$. If DDH is hard in $\mathbb{G}$, then distributions of tuples of these forms are indistinguishable. Since $\mathcal{H}^p$ is a random oracle whose output is independent of input, then distributions of tuples of the form $(rG, \mathcal{H}^p(rG), r''G)$ and $(rG, r'G, r''G)$ are identical. Similarly, distributions of tuples of the form $(rG, \mathcal{H}^p(rG), r\mathcal{H}^p(rG))$ and $(rG, \mathcal{H}^p(rG), r''G)$ are identical. Finally, random self-reducibility of the classic DDH game means that solving one instance of the problem has complexity no worse than solving a sequence of random instances of the problem.

Theorem. *If there exists a (t, ϵ, q)-solver of the linkable anonymity game of Definition 9 under the construction of Definition 10, then there exists a $(t + t', \epsilon/2, q)$-solver of the RO-DDH game for some t'.*

Proof. Let $\mathtt{A}$ be such a solver of the linkable anonymity game. We will construct an algorithm $\mathtt{B}$ that executes $\mathtt{A}$ in a black box and is a solver of the RO-DDH game, acting as the challenger for $\mathtt{A}$; the algorithm will pass on $\mathcal{H}^p$ random oracle queries to its own challenger, flip coins for $\mathcal{H}_0^s$ and $\{\mathcal{H}_j^s\}$ random oracle queries, and simulate signing oracle queries by backpatching. We assume that $\mathtt{B}$ keeps internal tables to maintain consistency between the random oracle queries needed to simulate signing oracle queries.

- $\mathtt{B}$ receives a set of tuples $\{(R_i, R'_i, R''_i)\}_{i=0}^{q-1}$ from its challenger, and chooses a bit $b' \in \{0,1\}$ uniformly at random. Note that $\mathtt{B}$ does not know if its tuples are RO-DDH triples or not, as its challenger chose a secret bit $b \in \{0,1\}$ uniformly at random to determine this.

- For all $i \in [0,q)$, $\mathtt{B}$ defines $X_i := R_i$ and records the $\mathcal{H}^p$ oracle mapping $\mathcal{H}^p(X_i) = R'_i$. It chooses $\{z_{i,j}\}_{j=1}^{d-1}$ from $\mathbb{F}_p$ uniformly at random, and builds a set of public keys $S := \{(X_i, z_{i,1}G, \ldots, z_{i,d-1}G)\}_{i=0}^{q-1}$. $\mathtt{B}$ provides the set S to $\mathtt{A}$.

- $\mathtt{A}$ returns indices i_0, i_0 to $\mathtt{B}$.

- $\mathtt{B}$ receives signing oracle queries of the form $\mathtt{SO}(m, Q, pk)$, where $0 \leq \ell < q$ is the index of $pk \in Q$, $pk \in S$, and $|Q| = n$. There are two cases, which determine how $\mathtt{B}$ simulates the oracle response, flipping coins for $\mathcal{H}_0^s$ and $\{\mathcal{H}_j^s\}$ oracle queries:
  - If it is the case that $\{pk_{i_0}, pk_{i_1}\} \not\subset Q$ or $pk \notin \{pk_{i_0}, pk_{i_1}\}$, then $\mathtt{B}$ proceeds with its signing oracle simulation using the key pk.
  - Otherwise, there exists a bit $c \in \{0,1\}$ such that $pk = pk_{i_c}$. In this case, $\mathtt{B}$ sets $c' := c \oplus b'$ and proceeds with its signing oracle simulation using the key $pk_{i_{c'}}$. This is, if $b' = 0$, then $\mathtt{B}$ simulates a signature using the requested key from the player-provided index set. If instead $b' = 1$, then $\mathtt{B}$ simulates a signature using the other key.

  In either case, $\mathtt{B}$ parses the public key set Q provided by $\mathtt{A}$. For any key $pk_i := (X'_i, Z'_{i,1}, \ldots, Z'_{i,d-1}) \in Q \setminus S$, it makes oracle queries to its challenger to obtain $\mathcal{H}^p(X'_i)$. Then $\mathtt{B}$ simulates the signature:
  - Define a map $\pi : [0,n) \to [0,q) \cup \{\perp\}$ that maps indices of elements of Q to the corresponding elements of S (or returns the distinguished failure symbol $\perp$ for indices not mapping to elements of S), and let $0 \leq \ell < n$ be the index of $pk \in Q$.
  - Choose $c_\ell, \{s_i\}_{i=0}^{n-1} \in \mathbb{F}_p$ uniformly at random.
  - Since $pk \in S$ by construction, $\pi(\ell) \neq \perp$. Set $\mathfrak{T} := R''_{\pi(\ell)}$ and $\{\mathfrak{D}_j\}_{j=1}^{d-1}$ such that each $\mathfrak{D}_j := z_{\pi(\ell),j}\mathcal{H}^p(X_{\pi(\ell)})$.
  - Define the following:

$$\begin{aligned} \mu_X &\leftarrow \mathcal{H}_0^s(Q, \mathfrak{T}, \{\mathfrak{D}_j\}) \\ \mu_j &\leftarrow \mathcal{H}_j^s(Q, \mathfrak{T}, \{\mathfrak{D}_j\}) \text{ for } j \in (0,d) \\ \mathfrak{W}_i &:= \begin{cases} \mu_X X_{\pi(i)} + \sum_j \mu_j Z_{\pi(i),j} & (\pi(i) \neq \perp) \\ \mu_X X'_i + \sum_j \mu_j Z'_{i,j} & (\pi(i) = \perp) \end{cases} \\ W &:= \mu_X \mathfrak{T} + \sum_j \mu_j \mathfrak{D}_j \end{aligned}$$

  - For each $i = \ell, \ell+1, \ldots, n-1, 0, \ldots, \ell-1$ (that is, indexing modulo n), define the following:

$$\begin{aligned} L_i &:= s_i G + c_i \mathfrak{W}_i \\ R_i &:= \begin{cases} s_i \mathcal{H}^p(X_{\pi(i)}) + c_i W & (\pi(i) \neq \perp) \\ s_i \mathcal{H}^p(X'_i) + c_i W & (\pi(i) = \perp) \end{cases} \\ c_{i+1} &\leftarrow \mathcal{H}_0^s(Q, m, L_i, R_i) \end{aligned}$$

  - $\mathtt{B}$ returns to $\mathtt{A}$ the tuple $(c_0, \{s_i\}, \mathfrak{T}, \{\mathfrak{D}_j\})$.

- $\mathtt{A}$ returns a bit b^* to $\mathtt{B}$.

- If $b^* = b'$, then $\mathtt{B}$ returns 0 to its challenger. Otherwise, it returns 1.

It is the case that $\mathtt{B}$ wins the RO-DDH game precisely when it correctly guesses the bit b chosen by its challenger; that is, when $b' = b$. Hence $\mathbb{P}[\mathtt{B} \text{ wins}] = \frac{1}{2}\mathbb{P}[\mathtt{B} \to 0 | b = 0] + \frac{1}{2}\mathbb{P}[\mathtt{B} \to 1 | b = 1]$.

If $b = 1$, then the RO-DDH challenger provided random points of the form R_i'' that $\mathtt{B}$ used in its signatures, so $\mathtt{A}$ can do no better than random chance at determining b'. Since $\mathtt{B} \to 1$ exactly when $\mathtt{A}$ loses the linkable anonymity game, we have $\mathbb{P}[\mathtt{B} \to 1 | b = 1] = \frac{1}{2}$.

On the other hand, if $b = 0$, then the RO-DDH challenger provided structured tuples that $\mathtt{B}$ used in its signatures, and $\mathtt{A}$ wins the linkable anonymity game with non-negligible advantage ϵ over random chance. Since $\mathtt{B} \to 0$ exactly when $\mathtt{A}$ wins the linkable anonymity game, we have $\mathbb{P}[\mathtt{B} \to 0 | b = 0] = \frac{1}{2} + \epsilon$.

This means $\mathtt{B}$ wins the RO-DDH game with probability $\mathbb{P}[\mathtt{B} \text{ wins}] = \frac{1}{2} + \frac{\epsilon}{2}$ and has advantage $\frac{\epsilon}{2}$. Further, $\mathtt{B}$ finishes with an added time t' used in simulating oracle queries and performing lookups. This means $\mathtt{B}$ is a $(t + t', \epsilon/2, q)$-solver of the RO-DDH game, where ϵ is non-negligible. $\square$