Post-quantum security of cryptographic transformations in the random oracle model

Huang, Y.

Appendix

A.1 Breaking a Weakened Phi-Non-Malleability

Following the (updated) definition in [CDF+23, Def. 2.4], a hash function H is Φ-non-malleable if for every pair $(\mathcal{D}, \mathcal{A})$ of PPT algorithms for which the HILL entropy $\mathsf{HILL}_\infty(x \mid \mathsf{st})$ is sufficiently large for $(\mathcal{X}, \mathsf{st}) \leftarrow \mathcal{D}$ and $x \leftarrow \mathcal{X}$, the probability of winning the game in Fig. A.1 is negligible. In case of a hash function family, the hash key is given as input to $\mathcal{D}$ and the HILL entropy is then also conditioned on the hash key. In case of H a random oracle, $\mathcal{D}$ is given query access to H and the entropy requirement is then on the statistical min-entropy $H_\infty(x \mid H, \mathsf{st})$, where one additionally conditions on the (function table of) the random oracle.

The relevant choice of Φ for the non-resignability claim in [CDF+23] is

$$\Phi = \{\phi_{\mathsf{pk}'} : (\mathsf{pk}, m) \mapsto (\mathsf{pk}', m) \,|\, \mathsf{pk}' \in \mathcal{PK}\}\,,$$

where $\mathcal{PK}$ is the space of all public keys. In more detail, [CDF+23, Lemma 5.7] shows that the considered NR property of the (original) BUFF transform is satisfied *if* the considered hash function H (or hash function family) satisfies the above notion of Φ-non-malleability for this particular choice of Φ.

$\Phi\text{-}\mathsf{NM}_0$:
1: $(\mathcal{X}, \mathsf{st}) \leftarrow \mathcal{D}$
2: $x \leftarrow \mathcal{X}$
3: $y := H(x)$
4: $(y', \phi) \leftarrow \mathcal{A}(y, \mathsf{st})$
5: **return** $(\, H(\phi(x)) = y' \,\wedge\, \phi(x) \neq x \,)$

Figure A.1: The Φ-non-malleability game, as considered in [CDF+23], but for a fixed hash function H. $\mathcal{X}$ is an efficiently sampleable distribution. The subscript in $\Phi\text{-}\mathsf{NM}_0$ here is meant to distinguish it from the original definition, which considers some additional auxiliary information.

We show here a simple attack against this notion of Φ-non-malleability for this choice of Φ. The attack applies to *any* hash function (family) H, including the random oracle, and so renders the non-resignability claim in [CDF+23, Lemma 5.7], and in [CDF+23, Theorem 5.5], vacuous.

The attack works as follows. $\mathcal{D}$ outputs the distribution $\mathcal{X}$ that samples a random $\mathsf{pk} \in \mathcal{PK}$ and outputs $x = (\mathsf{pk}, 0)$, and $\mathcal{A}$ ignores its input $y = H(\mathsf{pk}, 0)$ and simply outputs $(H(\mathsf{pk}', 0), \phi_{\mathsf{pk}'})$ for an arbitrary (fixed) $\mathsf{pk}' \in \mathcal{PK}$. Note that there is no state information st here, and the entropy condition is satisfied (assuming $\mathcal{PK}$ to be sufficiently large). Thus, this is a valid attack that succeeds with probability almost 1; it only fails when the random $\mathsf{pk} \in \mathcal{PK}$ happens to be pk'.

A.2 A Modified Measure-and-Reprogram Lemma

In [DFM20] we find the "measure-and-reprogram technique 2.0" (Theorem 2):

Theorem A.1 (Measure-and-reprogram)**.** *Let $\mathcal{X}$ and $\mathcal{Y}$ be finite non-empty sets. There exists a black-box two-stage quantum algorithm $\mathcal{S}$ with the following property. Let $\mathcal{A}$ be an arbitrary oracle quantum algorithm that makes q queries to a uniformly random $H : \mathcal{X} \to \mathcal{Y}$ and that outputs some $x \in \mathcal{X}$ and a (possibly quantum) output z. Then, the two-stage algorithm $\mathcal{S}^{\mathcal{A}}$ outputs some $x \in \mathcal{X}$ in the first stage and, upon a random $\Theta \in \mathcal{Y}$ as input to the second stage, a (possibly quantum) output z, so that for any $x_\circ \in \mathcal{X}$ and any (possibly quantum) predicate V:*

$$\Pr_{H,\Theta}\left[x = x_\circ \wedge V(x, \Theta, z) : (x, z) \leftarrow \langle \mathcal{S}^{\mathcal{A}}, \Theta \rangle\right] \geq \frac{1}{(2q+1)^2} \Pr_{H}\left[x = x_\circ \wedge V(x, H(x), z) : (x, z) \leftarrow \mathcal{A}^{H}\right].$$

Furthermore, $\mathcal{S}$ runs in time polynomial in q, $\log|\mathcal{X}|$, and $\log|\mathcal{Y}|$.

Here $\langle \mathcal{S}^{\mathcal{A}}, \Theta \rangle$ works as follows: First, one of the $q+1$ queries of $\mathcal{A}$ (also counting the final output in register X) is measured, and the measurement outcome x is output by (the first stage of) $\mathcal{S}$. Each of the q actual queries is picked with probability $\frac{2}{2q+1}$, while the final output is picked with probability $\frac{1}{2q+1}$. Then this very query of $\mathcal{A}$ is answered either using the original H *or* using the reprogrammed oracle $H{*}\Theta x$, with the choice being made at random[1], while all the remaining queries of $\mathcal{A}$ are answered using oracle $H{*}\Theta x$. Finally, (the second stage of) $\mathcal{S}$ outputs whatever $\mathcal{A}$ outputs.

The theorem follows directly from the above definition of $\mathcal{S}$ and a technical lemma. Let first $|\phi_i\rangle$ be defined as $\mathcal{A}$'s state right before making its $i+1$st

[1] If it is the final output that is measured then there is nothing left to reprogram, so no choice has to be made.

query — with the special case $|\phi_q\rangle$ denoting the final output state — to which we add the superscript $\mathcal{O} \in \{H, H*\Theta x\}$ when all previous queries have been answered using $\mathcal{O}$. Next, we use $\mathcal{A}^{\mathcal{O}}_{i\to j}$ to denote the unitary that brings $\mathcal{A}$ from $|\phi_i\rangle$ to $|\phi_j\rangle$, using $\mathcal{O}$ from the ith query on. Finally, we use the shorthand $X := |x\rangle\langle x|$. The lemma then reads:

Lemma A.2. *Let $\mathcal{A}$ be a q-query oracle quantum algorithm. Then, for any function $H : \mathcal{X} \to \mathcal{Y}$, any $x \in \mathcal{X}$ and $\Theta \in \mathcal{Y}$, and any projection $\Pi_{x,\Theta}$, it holds that*

$$\mathbb{E}_{i,b}\left[\left\|(X \otimes \Pi_{x,\Theta})\big(\mathcal{A}^{H*\Theta x}_{i+b\to q}\big)\big(\mathcal{A}^{H}_{i\to i+b}\big)X\left|\phi^H_i\right\rangle\right\|_2^2\right] \geq \frac{\left\|(X \otimes \Pi_{x,\Theta})\left|\phi^{H*\Theta x}_q\right\rangle\right\|_2^2}{(2q+1)^2},$$

where the expectation is over uniform $(i, b) \in (\{0, \ldots, q-1\} \times \{0, 1\}) \cup \{(q, 0)\}$.

Here the left-hand side corresponds to the success probability of $\mathcal{S}$ with respect to V and Θ, while (in expectation over Θ) the right-hand side is equal to the success probability of the adversary in a normal run, now with respect to V and the original oracle output $H(x)$.

A first observation is that the technical lemma actually proves something slightly stronger than Theorem A.1; If we let $\mathcal{S}$ additionally output the measurement outcome x, we get the condition $x = x'$ for free (since the same projector X is used on the query as well as the final output state). On the other hand, for our application it suffices to use a slightly weaker statement (in a different respect) that we obtain by summing over all $x_\circ \in \mathcal{X}$:

$$\begin{aligned}&\Pr_{\Theta}\big[x = x' \wedge V(x, \Theta, z) : (x, x', z) \leftarrow \langle \mathcal{S}^{\mathcal{A}}, \Theta\rangle\big]\\ &\geq \frac{1}{(2q+1)^2}\Pr_{H}\big[V(x, H(x), z) : (x, z) \leftarrow \mathcal{A}^H\big].\end{aligned}$$

Next, we will reduce q to account for only those queries where $\mathcal{S}$ has a non-zero probability of measuring the same $x' = x$ that will eventually be output by $\mathcal{A}$, while also satisfying the quantum predicate. The probability here is over the choice of H, Θ and the measurement outcome x', we thus define:

$$\begin{aligned}Q_{\min} := \{i \in \{0, \ldots, q-1\} \mid \exists H \in \mathcal{Y}^{\mathcal{X}}, \exists \Theta \in \mathcal{Y}, \exists x \in \mathcal{X}, \exists b \in \{0, 1\} \text{ s.t.}\\ \left\|(X \otimes \Pi_{x,\Theta})\big(\mathcal{A}^{H*\Theta x}_{i+b\to q}\big)\big(\mathcal{A}^{H}_{i\to i+b}\big)X\left|\phi^H_i\right\rangle\right\|_2 \neq 0\}.\end{aligned}$$

Let furthermore Q be any subset of queries such that $Q_{\min} \subseteq Q \subseteq \{0, \ldots, q-1\}$. It will now be easy to prove the following modified lemma:

Lemma A.3. *Let $\mathcal{A}$ be a q-query oracle quantum algorithm, with Q as defined above. Then, for any function $H\colon \mathcal{X} \to \mathcal{Y}$, any $x \in \mathcal{X}$ and $\Theta \in \mathcal{Y}$, and any*

projection $\Pi_{x,\Theta}$*, it holds that*

$$\mathbb{E}_{i,b}\left[\left\|(X\otimes\Pi_{x,\Theta})\left(\mathcal{A}^{H*\Theta x}_{i+b\to q}\right)\left(\mathcal{A}^{H}_{i\to i+b}\right)X\left|\phi^H_i\right\rangle\right\|_2^2\right]\geq\frac{\left\|(X\otimes\Pi_{x,\Theta})\left|\phi^{H*\Theta x}_q\right\rangle\right\|_2^2}{(2|Q|+1)^2}\,,$$

where the expectation is over uniform $(i,b)\in(Q\times\{0,1\})\cup\{(q,0)\}$*.*

Note that the only difference to Lemma A.2 is in the expectation on the left-hand side and the denominator on the right-hand side, as indicated in blue. The proof is largely taken from [DFM20], with a small modification which we highlight with a yellow background.

Proof. For any $0\leq i\leq q$, inserting a resolution of the identity and exploiting that

$$\left(\mathcal{A}^{H*\Theta x}_{i+1\to q}\right)\left(\mathcal{A}^{H}_{i\to i+1}\right)(\mathbb{I}-X)\left|\phi^H_i\right\rangle=\left(\mathcal{A}^{H*\Theta x}_{i\to q}\right)(\mathbb{I}-X)\left|\phi^H_i\right\rangle\,,$$

we can write

$$\begin{aligned}
&\left(\mathcal{A}^{H*\Theta x}_{i+1\to q}\right)\left|\phi^H_{i+1}\right\rangle\\
&\quad=\left(\mathcal{A}^{H*\Theta x}_{i+1\to q}\right)\left(\mathcal{A}^{H}_{i\to i+1}\right)(\mathbb{I}-X)\left|\phi^H_i\right\rangle &&+\left(\mathcal{A}^{H*\Theta x}_{i+1\to q}\right)\left(\mathcal{A}^{H}_{i\to i+1}\right)X\left|\phi^H_i\right\rangle\\
&\quad=\left(\mathcal{A}^{H*\Theta x}_{i\to q}\right)(\mathbb{I}-X)\left|\phi^H_i\right\rangle &&+\left(\mathcal{A}^{H*\Theta x}_{i+1\to q}\right)\left(\mathcal{A}^{H}_{i\to i+1}\right)X\left|\phi^H_i\right\rangle\\
&\quad=\left(\mathcal{A}^{H*\Theta x}_{i\to q}\right)\left|\phi^H_i\right\rangle-\left(\mathcal{A}^{H*\Theta x}_{i\to q}\right)X\left|\phi^H_i\right\rangle &&+\left(\mathcal{A}^{H*\Theta x}_{i+1\to q}\right)\left(\mathcal{A}^{H}_{i\to i+1}\right)X\left|\phi^H_i\right\rangle
\end{aligned}$$

Rearranging terms, applying $G^{\Theta}_x=(X\otimes\Pi_{x,\Theta})$ and using the triangle equality, we can thus bound

$$\begin{aligned}
\left\|G^{\Theta}_x\left(\mathcal{A}^{H*\Theta x}_{i\to q}\right)\left|\phi^H_i\right\rangle\right\|_2\leq{}&\left\|G^{\Theta}_x\left(\mathcal{A}^{H*\Theta x}_{i+1\to q}\right)\left|\phi^H_{i+1}\right\rangle\right\|_2\\
&+\left\|G^{\Theta}_x\left(\mathcal{A}^{H*\Theta x}_{i\to q}\right)X\left|\phi^H_i\right\rangle\right\|_2\\
&+\left\|G^{\Theta}_x\left(\mathcal{A}^{H*\Theta x}_{i+1\to q}\right)\left(\mathcal{A}^{H}_{i\to i+1}\right)X\left|\phi^H_i\right\rangle\right\|_2.
\end{aligned}$$

Summing up the respective sides of the inequality over $i=0,\ldots,q-1$, dropping (some of) the zero terms in the summation[2], we get

$$\left\|G^{\Theta}_x\left|\phi^{H*\Theta x}_q\right\rangle\right\|_2\;\leq\;\left\|G^{\Theta}_x\left|\phi^H_q\right\rangle\right\|_2+\sum_{\substack{i\in Q\\ b\in\{0,1\}}}\left\|G^{\Theta}_x\left(\mathcal{A}^{H*\Theta x}_{i+b\to q}\right)\left(\mathcal{A}^{H}_{i\to i+b}\right)X\left|\phi^H_i\right\rangle\right\|_2.$$

By squaring both sides, dividing by $2|Q|+1$ (i.e., the number of terms on the right-hand side), and using Jensen's inequality on the right-hand side, we

[2] At most (if $Q=Q_{\min}$) we drop all terms that are zero for every choice of b, H, Θ, and x.

obtain

$$\frac{\left\|G_x^\Theta\left|\phi_q^{H*\Theta x}\right\rangle\right\|_2^2}{2|Q|+1} \leq \left\|G_x^\Theta\left|\phi_q^H\right\rangle\right\|_2^2 + \sum_{\substack{0\leq i<q\\ b\in\{0,1\}}} \left\|G_x^\Theta\left(\mathcal{A}_{i+b\to q}^{H*\Theta x}\right)\left(\mathcal{A}_{i\to i+b}^{H}\right)X\left|\phi_i^H\right\rangle\right\|_2^2$$

and thus, noting that we can write $\left\|G_x^\Theta\left|\phi_q^H\right\rangle\right\|_2^2$ as

$$\left\|G_x^\Theta\left(\mathcal{A}_{i+b\to q}^{H*\Theta x}\right)\left(\mathcal{A}_{i\to i+b}^{H}\right)X\left|\phi_i^H\right\rangle\right\|_2^2$$

with $i=q$ and $b=0$,

$$\frac{\left\|G_x^\Theta\left|\phi_q^{H*\Theta x}\right\rangle\right\|_2^2}{(2|Q|+1)^2} \;\leq\; \mathbb{E}_{i\in Q,b}\left[\left\|G_x^\Theta\left(\mathcal{A}_{i+b\to q}^{H*\Theta x}\right)\left(\mathcal{A}_{i\to i+b}^{H}\right)X\left|\phi_i^H\right\rangle\right\|_2^2\right].$$

This concludes the proof. □

The corresponding theorem reads as follows:

Theorem A.4 (Measure-and-reprogram with stingy simulator)**.** *Let $\mathcal{X}$ and $\mathcal{Y}$ be finite non-empty sets. There exists a black-box two-stage quantum algorithm $\mathcal{S}$ with the following property. Let $\mathcal{A}$ be an arbitrary oracle quantum algorithm that makes q queries to a uniformly random $H:\mathcal{X}\to\mathcal{Y}$ and that outputs some $x\in\mathcal{X}$ and a (possibly quantum) output z, and let V be a (possibly quantum) predicate. For $i\in\{0,\ldots,q-1\}$, define the two-stage algorithm $\mathcal{S}_i^{\mathcal{A}}$ as follows: In the first stage $\mathcal{S}_i$ measures the ith query of $\mathcal{A}$, and outputs the measurement outcome x'. Then, upon a random $\Theta\in\mathcal{Y}$ as input to the second stage, this very query of $\mathcal{A}$ is answered either using the original H* or *using the reprogrammed oracle $H*\Theta x$, with the choice being made at random, while all the remaining queries of $\mathcal{A}$ are answered using oracle $H*\Theta x$. At the end of its run $\mathcal{S}_i$ then outputs whatever $\mathcal{A}$ outputs (along with i). Now let $Q\subseteq\{0,\ldots,q-1\}$ be such that for all $i\notin Q$ we have $\Pr_{H,\Theta}\left[x'=x\wedge V(x,\Theta,z):(x',x,z)\leftarrow\langle\mathcal{S}_i^{\mathcal{A}},\Theta\rangle\right]=0$. Define $\mathcal{S}(Q)$ to be the algorithm that with probability $\frac{2|Q|}{2|Q|+1}$ picks i uniformly at random from Q and then runs $\mathcal{S}_i$, and with probability $\frac{1}{2|Q|+1}$ chooses $i=q$ and just simulates $\mathcal{A}$ without any measurement or reprogramming, and again outputs whatever $\mathcal{A}$ outputs (along with $x':=x$ and i). We then have*

$$\begin{aligned}&\Pr_{H,\Theta}\left[x'=x\wedge V(x,\Theta,z):(x',x,z,i)\leftarrow\langle\mathcal{S}^{\mathcal{A}}(Q),\Theta\rangle\right]\\ &\geq\frac{1}{(2|Q|+1)^2}\Pr_H\left[V(x,H(x),z):(x,z)\leftarrow\mathcal{A}^H\right].\end{aligned}$$

Furthermore, $\mathcal{S}$ runs in time polynomial in q, $\log|\mathcal{X}|$, and $\log|\mathcal{Y}|$.

A.3 Unsimplified Proof of Lemma 4.32

In this section, we explain how the proof of Lemma 4.32 presented in Section 4.7.2 can be modified to take into account the padding as well as the possibility that the lengths of the message and the public keys may not be multiples of the block length. The parts that change in comparison to Section 4.7.2 are marked in colour.

Lemma 4.32. *Let $\mathcal{D}^H$ and $\mathcal{A}^H$ be $\mathsf{sNR}^{H,\perp}$-adversaries against $\mathsf{sBUFF}[\mathcal{S},\mathsf{MD}]$, making at most $q_\mathcal{D}$ and $q_\mathcal{A} \in \mathbb{Z}_{>0}$ classical queries to H respectively; let $\mathsf{aux} : \mathcal{SK} \times \mathcal{M} \to \mathcal{AUX}$ be any (possibly randomized) function. Then there exists a hider $\bar{\mathcal{D}} : \{\perp\} \to \mathcal{X}^{\leq \bar{B}} \times \mathcal{Z}$ and a seeker $\bar{\mathcal{A}} : \mathcal{Y} \times \mathcal{Z} \to \mathcal{X}^{\leq \bar{B}}$ and $\mathcal{Z} = \mathcal{SK} \times \mathcal{AUX}$, where $\bar{\mathcal{A}}$ makes at most $q_\mathcal{B} := q_\mathcal{A} + q_\mathcal{S}$ and $\bar{\mathcal{D}}$ makes at most $q_\mathcal{D}$ queries to H, and such that*

$$\mathsf{H}^{\infty}_{(x,z)\leftarrow\bar{\mathcal{D}}^H}(x \mid H, z) = \mathsf{H}^{\infty}_{\substack{(\mathsf{sk},\mathsf{pk})\leftarrow\mathsf{KGen}^H \\ m\leftarrow\mathcal{D}^H(\mathsf{sk})}}(m \mid H, \mathsf{sk}, \mathsf{aux}(\mathsf{sk}, m)) \tag{4.22}$$

and $\mathbf{Adv}^{\mathsf{sNR}^{H,\perp}}_{\mathsf{sBUFF}[\mathcal{S},\mathsf{MD}]}(\mathcal{D}, \mathcal{A}, \mathsf{aux})$

$$\leq 2q_\mathcal{B} \cdot r^2 \cdot \mathbf{Adv}^{\mathsf{HnS}^H}_{\mathsf{MD}_\perp}(\bar{\mathcal{D}}, \bar{\mathcal{A}}) + \frac{(q_\mathcal{D}^2 \cdot r + 1) \cdot \bar{B}\bar{L} + q_\mathcal{D} + 2\bar{L}^2}{|\mathcal{Y}|}. \tag{4.23}$$

where $\bar{B}$ and $q_\mathcal{S}$ are as described in Section 4.7.1 and $\bar{L} = q_\mathcal{D} + q_\mathcal{A} + q_\mathcal{S} + 2\bar{B}$. Moreover, if aux is polynomial-time computable and $\mathcal{D}, \mathcal{A}$ are PPT, then so are $\bar{\mathcal{D}}, \bar{\mathcal{A}}$.

Proof. We explain the notation needed for the generalized proof where the lengths of messages and keys do not necessarily line up with the blocks. First, we note that

$$\mathbf{Adv}^{\mathsf{sNR}^{H,\perp}}_{\mathsf{sBUFF}[\mathcal{S},\mathsf{MD}_\perp]}(\mathcal{D}, \mathcal{A}, \mathsf{aux}) \leq \Pr\left[\mathsf{MD}^H_\perp(m\|\mathsf{pk}'\|m) = y' \wedge \mathsf{pk}' \neq \mathsf{pk}\right]$$

with the random variables $\mathsf{pk}, \mathsf{pk}', m$ and y defined by the experiment

$$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}, \quad m \leftarrow \mathcal{D}^H(\mathsf{sk}),$$
$$(\mathsf{pk}', y') \leftarrow \mathcal{B}^H\big(\mathsf{sk}, \mathsf{MD}^H(m\|\mathsf{pk}\|m), \mathsf{aux}(\mathsf{sk}, m)\big)$$

where $\mathcal{B}(\mathsf{sk}, y, a) := \mathcal{A}^H\big(\mathsf{sk}, (\mathsf{Sign}^H(\mathsf{sk}, y), y), a\big)$. We note that the random choice of H is understood and left implicit. We recall that $\mathcal{D}$ and $\mathcal{B}$ make at most $q_\mathcal{D}$ and $q_\mathcal{B} := q_\mathcal{A} + q_S$ queries to the random oracle respectively. We introduce the following additional random variables, implicitly defined by the above experiment.

Parsing $x = m\|\mathsf{pk}\|m\|\mathsf{pad}(m\|\mathsf{pk}\|m)$ as $x = (x_1, \ldots, x_{|x|_{\mathrm{bl}}})$ and $x' = m\|\mathsf{pk}'\|m\|\mathsf{pad}(m\|\mathsf{pk}'\|m)$ as $x' = (x'_1, \ldots, x'_{|x'|_{\mathrm{bl}}})$ and denoting by $B_{\mathsf{pk}'} =$

$|\,m\|\mathsf{pk}'\|m\|\mathsf{pad}(m\|\mathsf{pk}'\|m)\,|_{\mathrm{bl}}$ and by $B_{\mathsf{pk}} = |\,m\|\mathsf{pk}\|m\|\mathsf{pad}(m\|\mathsf{pk}\|m)\,|_{\mathrm{bl}}$, we let

$$B_1'' = |\,m\,|_{\mathrm{bl}}$$

and

$$B_2'' = \begin{cases} B_{\mathsf{pk}'} - |\,m\|\mathsf{pk}'\,|_{\mathrm{bl}} & \text{if } |\,m\|\mathsf{pk}'\,| = |\,m\|\mathsf{pk}'\,|_{\mathrm{bl}} \cdot r \\ B_{\mathsf{pk}'} - |\,m\|\mathsf{pk}'\,|_{\mathrm{bl}} + 1 & \text{otherwise} \end{cases}$$

i.e., B_1'' is the number of blocks that contain the first occurrence of m, and B_2'' is the number of blocks that contain the second occurrence of m in the sandwich $m\|\mathsf{pk}'\|m$.

For $i \in [B_1'']$ we define m_i to be the ith block of $m\|\mathsf{pk}'$, and for $i \in [B_2'']$ we define m_i' to be the ith block starting from the beginning of the second occurrence of m in the sandwich $m\|\mathsf{pk}'\|m\|\mathsf{pad}(m\|\mathsf{pk}'\|m)$. We define

$$z_1' := \mathsf{MD}_{\perp}^{H}(x_1'\|\ldots\|x'_{B-B_2''}) \text{ and } z'_{i+1} := \mathsf{MD}_{\perp}^{H}(x_1'\|\ldots\|x'_{B-B_2''+i}) = H(m_i', z_i')$$

for $i = 1, \ldots, B_2''$, with $z_{B_2''+1} = \mathsf{MD}^H(m\|\mathsf{pk}'\|m)$ then. The z_i's thus form the "high-order" intermediate digests towards computing $\mathsf{MD}^H(m\|\mathsf{pk}'\|m)$.[3]

Finally, we let $\tau_1, \ldots, \tau_L$ with $L = q_{\mathcal{D}} + B_{\mathsf{pk}} + q_{\mathcal{B}} + B_{\mathsf{pk}'}$ be the list of inputs to all the hash computations performed during the experiment, listed in the performed order; see Fig. 4.18b. Hence, $Q_{\mathcal{D}} = \{\tau_1, \ldots, \tau_{q_{\mathcal{D}}}\}$ consists of the hash queries made by $\mathcal{D}$, we denote by $Q_{\mathsf{MD}(m\|\mathsf{pk}\|m)}$ the B_{pk} queries made during the computation of $\mathsf{MD}(m\|\mathsf{pk}\|m)$ by the challenger, and $Q_{\mathcal{B}} = \{\tau_{q_{\mathcal{D}}+B_{\mathsf{pk}}+1}, \ldots, \tau_{q_{\mathcal{D}}+B_{\mathsf{pk}}+q_{\mathcal{B}}}\}$ of the queries made by $\mathcal{B}$, and the remaining τ_ℓ's are the inputs to the hash computations done towards computing $\mathsf{MD}^H(m\|\mathsf{pk}'\|m)$, in particular $\tau_{q_{\mathcal{D}}+B_{\mathsf{pk}}+q_{\mathcal{B}}+B_{\mathsf{pk}'}-B_2''+1} = (m_1', z_1')$, and $\tau_{q_{\mathcal{D}}+B_{\mathsf{pk}}+q_{\mathcal{B}}+B_{\mathsf{pk}'}-B_2''+2} = (m_2', z_2')$, etc. For any τ_ℓ with $\ell \in [L]$, we write $\mathsf{R}(\tau_\ell)$ for the right component of τ_ℓ, i.e., $\mathsf{R}(\tau_{q_{\mathcal{D}}+B_{\mathsf{pk}}+q_{\mathcal{B}}+B_{\mathsf{pk}'}-B_2''+1}) = z_1'$, etc. and $\mathsf{L}(\tau_\ell)$ is the left component of τ_ℓ, i.e. $\mathsf{L}(\tau_{q_{\mathcal{D}}+B_{\mathsf{pk}}+q_{\mathcal{B}}+B_{\mathsf{pk}'}-B_2''+1}) = m_1'$ etc.

As explained, we are interested in upper-bounding the probability $\Pr[\Sigma]$ of the event

$$\Sigma := \left[\mathsf{MD}^H(m\|\mathsf{pk}'\|m) = y' \wedge \mathsf{pk}' \neq \mathsf{pk}\right].$$

We do this by introducing a sequence of further events, Γ, Λ and Δ, with the property that $\Pr[\Sigma]$ is close to $\Pr[\Sigma \wedge \Gamma \wedge \Lambda \wedge \Delta]$, assuming $\mathbf{Adv}^{\mathsf{HnS}^H_{\mathsf{MD}_\perp}}(\bar{\mathcal{D}}, \bar{\mathcal{A}})$ is small (for suitable choices of $\bar{\mathcal{D}}$ and $\bar{\mathcal{A}}$), and such that we can upper bound the latter probability.

We start off avoiding some atypical behavior of H. Formally, we consider

[3] By "high-order" we mean the digests occurring in the computation of $\mathsf{MD}^H(m\|\mathsf{pk}'\|m)$ from $\mathsf{MD}_{\perp}^{H}(m\|\mathsf{pk}')$.

the good event $\Gamma := \Gamma_1 \wedge \Gamma_2 \wedge \Gamma_3$ with

$$\Gamma_1 := \left[\forall\, \ell, \ell' \in [L] : H(\tau_\ell) = H(\tau_{\ell'}) \;\Rightarrow\; \tau_\ell = \tau_{\ell'}\right]$$
$$\Gamma_2 := \left[\forall\, \ell, \ell' \in [L] : H(\tau_\ell) = \mathsf{R}(\tau_{\ell'}) \;\Rightarrow\; (\exists\, \ell_\circ < \ell' : \tau_\ell = \tau_{\ell_\circ})\right] \qquad \text{and}$$
$$\Gamma_3 := \left[\forall\, \ell \in [q_{\mathcal{D}}] : H(\tau_\ell) \neq IV\right]$$

Informally, Γ_1 states that there are no collisions for the points that H was queried on, Γ_2 states that a hash output does not "bump into" a previous hash input, thus retroactively connecting hash chains, and lastly, Γ_3 states that the initialization vector is never a hash output (this will be helpful later on to identify the start of a hash chain). These events are defined identically as in Section 4.7.2.

Claim 4.33. *It holds that* $\Pr[\Sigma] \leq \Pr[\Sigma \wedge \Gamma] + q_{\mathcal{D}}/|\mathcal{Y}| + 2\bar{L}^2/|\mathcal{Y}|$.

The proof of this claim is identical as that presented in Section 4.7.2.

To bound $\Sigma \wedge \neg\mathsf{GD}$, we need to adapt the subevents $\Delta, \Delta'_k, \Delta^i$ to the new setting.

First, we adapt the event Λ from Section 4.7.2 to the notation above. The goal is to show that if $\mathcal{B}$ has not queried the entire hash chain of the computation of $\mathsf{MD}(m\|\mathsf{pk}'\|m)$,

$$\Lambda := [\exists i\colon (m'_i, z'_i) \notin Q_{\mathcal{B}}]$$

that $\mathcal{B}$ has not made a hash query to one of the high-order intermediate digests z'_i, together with the corresponding message block m'_i.

Claim 4.34. *There exist hide-and-seek adversaries* $\bar{\mathcal{D}}, \bar{\mathcal{A}}$ *such that*

$$\Pr[\Sigma \wedge \Gamma \wedge \neg\Lambda] \leq q_{\mathcal{B}} \cdot 2r^2 \cdot \mathbf{Adv}^{\mathsf{HnS}^H_{\mathsf{MD}_\perp}}(\bar{\mathcal{D}}, \bar{\mathcal{A}})\,, \tag{4.25}$$

where $\bar{\mathcal{A}}$ *makes at most* $q_{\mathcal{B}}$ *and the value* x *chosen by* $\bar{\mathcal{D}}$ *preserves the entropy:*

$$\mathsf{H}_\infty(x \mid z, H) = \mathsf{H}_\infty(m \mid H, \mathsf{sk}, \mathsf{aux}(\mathsf{sk}, m))\,.$$

Moreover, aux *is polynomial-time computable and* $\mathcal{D}, \mathcal{A}$ *are PPT, then so are* $\bar{\mathcal{D}}$ *and* $\bar{\mathcal{A}}$.

Proof. We construct adversaries $\bar{\mathcal{D}}$ and $\bar{\mathcal{A}}$ against hide and seek. First, the adversary $\bar{\mathcal{D}}$ simulates the sNR game to $\mathcal{D}$ by sampling a key pair $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}$ and giving sk to $\mathcal{D}$. It forwards all queries and responses by $\mathcal{D}$ to the random oracle and back. When $\mathcal{D}$ outputs a message m, the adversary $\bar{\mathcal{D}}$ outputs $x = m\|\mathsf{pk}\|m\|\mathsf{pad}(m\|\mathsf{pk}\|m)$ and $z = \mathsf{sk}, \mathsf{aux}(\mathsf{sk}, m)$ as its output.

The adversary $\bar{\mathcal{A}}$ takes as input the hash y and $z = \mathsf{sk}, \mathsf{aux}(\mathsf{sk}, m)$. It parses z into sk and $\mathsf{aux}(\mathsf{sk}, m)$ and runs $\mathcal{B}$ on $\mathsf{sk}, y, \mathsf{aux}(\mathsf{sk}, m)$. It forwards all queries to H and their responses. Here, we observe that if Γ and Σ hold but Λ does not hold, then $\bar{\mathcal{A}}$ is able to restore the entire message m (and

thus win the corresponding hide-and-seek game against $\mathsf{MD}_\perp$ by computing $m\|\mathsf{pk}\|m\|\mathsf{pad}(m\|\mathsf{pk}\|m))$, via inspecting $\mathcal{B}$'s queries to H and its output y' as follows. Indeed, $z'_{B''_2+1} = y'$ (by Σ), and $\mathcal{B}$ has queried $(m'_{B''_2}, z'_{B''_2})$ such that $H(m'_{B''_2}, z'_{B''_2}) = z'_{B''_2+1} = y'$ (by $\neg\Lambda$), and $(m'_{B''_2}, z'_{B''_2})$ is unique with that property (by Γ_1), and so $\bar{\mathcal{A}}$ can find it. By the same argument, $\bar{\mathcal{A}}$ can then find $(m'_{B''_2-1}, z'_{B''_2-1}), (m'_{B''_2-2}, z'_{B''_2-2}), \ldots, (m'_1, z'_1)$ in the queries if it knows B''_2, which is at most $q_{\mathcal{B}}$ and can be guessed with probability $1/q_{\mathcal{B}}$. It remains to guess where the message starts within the block m'_1, which $\bar{\mathcal{A}}$ can guess with probability $\frac{1}{r}$ The adversary $\bar{\mathcal{A}}$ then identifies the padding at the end of the string. If the padding is not easily identifiable, the adversary $\bar{\mathcal{A}}$ makes a guess of the length of the padding which succeeds with probability $\frac{1}{2r}$ as the padding is at most $2r$ long. □

It remains to to bound the success probability of the adversaries in the case that Λ holds.

To define the event Δ analogously to Section 4.7.2 we define m'_i for $i = 0, -1, -2\ldots$ to be the first, second, third ... block before m'_1. Analogously we define z'_i to be the corresponding intermediate digest. We define

$$\Delta := \left[\exists i \geq -\left|\, m\|\mathsf{pk}'\,\right|_{\mathrm{bl}} + B''_1 \colon (m'_i, z'_i) \notin Q_{\mathcal{B}} \cup Q_{\mathcal{D}} \cup Q_{\mathsf{MD}(m\|\mathsf{pk}\|m)}\right]$$

and

$$\Delta'_k := \left[\exists i \in [B''_2] \colon \tau_k = (m'_i, z'_i) \notin Q_{\mathcal{B}} \cup Q_{\mathsf{MD}_\perp(m\|\mathsf{pk}\|m)} \cup \{\tau_{k'}\}_{k' \leq k}\right]$$

for $k \in \{1, \ldots, q_{\mathcal{D}}\}$. It is not too hard to see that $\Delta \vee \Delta'_1 \vee \ldots \vee \Delta'_{q_{\mathcal{D}}} \Leftarrow \Sigma \wedge \Gamma \wedge \Lambda$, and thus by basic manipulations

$$\Pr[\Sigma] \leq \Pr[\Sigma \wedge \Delta] + \sum_k \Pr[\Sigma \wedge \Gamma \wedge \Delta'_k] + \Pr[\Sigma \wedge \Gamma \wedge \neg\Lambda] + \Pr[\neg\Gamma]\,,$$

where we already have bounds for the last two terms.

First, we argue that $\Pr[\Sigma \wedge \Delta]$ is small. For that purpose, we introduce

$$\Delta^i := \left[i \leq B_{\mathsf{pk}'} - B''_1 + 1 \wedge (m'_{B''_2-i+1}, z_{B''_2-i+1}) \notin Q_{\mathcal{B}} \cup Q_{\mathcal{D}} \cup Q_{\mathsf{MD}(m\|\mathsf{pk}\|m)}\right]$$

where $\Delta^{>i} = \bigvee_{j=i+1}^{\bar{B}} \Delta^j$. We note that if $B''_1 \cdot r = |\, m\,|$ then $\Delta^{B_{\mathsf{pk}'} - B''_1 + 1}$ will always be false as the query will happen during the computation of $\mathsf{MD}(m\|\mathsf{pk}\|m)$.

$$\Pr[\Sigma \wedge \Delta] \leq \sum_{i=1}^{\bar{B}} \Pr\left[\Sigma \wedge \Delta^i \wedge \neg\Delta^{>i}\right].$$

The crucial observation now is that conditioned on Δ^i, the hash value of $z'_{B''_2-i+2} = H(m'_{B''_2-i+1}, z_{B''_2-i+1}{}')$ is uniformly random and independent of

y' (and of "everything else"). We formalize this in the claim below, and when plugging in the numbers we obtain:

$$\begin{aligned}\Pr[\Sigma \wedge \Delta] &\leq \sum_{i\in[\bar{B}]} \Pr\left[\Sigma \wedge \Delta^i \wedge \neg\Delta^{>i}\right] \\ &= 0 + \sum_{\substack{i\in[\bar{B}] \text{ s.t.} \\ \Pr[\Delta^i\wedge\neg\Delta^{>i}]>0}} \Pr\left[\Sigma \wedge \Delta^i \wedge \neg\Delta^{>i}\right] \cdot \Pr\left[\Sigma \;\middle|\; \Delta^i \wedge \neg\Delta^{>i}\right] \\ &\leq \sum_{\substack{i\in[\bar{B}] \text{ s.t.} \\ \Pr[\Delta^i\wedge\neg\Delta^{>i}]>0}} \Pr\left[\Delta^i \wedge \neg\Delta^{>i}\right] \cdot \bar{B}\bar{L}/|\mathcal{Y}| \;\leq \bar{B}\bar{L}/|\mathcal{Y}|\;,\end{aligned}$$

where $\bar{L} := q_{\mathcal{D}} + \bar{B} + q_{\mathcal{B}} + \bar{B}$, and the last inequality follows by the disjointness of $\Delta^i \wedge \neg\Delta^{>i}$ across $i \in [\bar{B}]$.

We restate the bound on Δ^i:

Claim 4.35. *It holds for every $i \in [\bar{B}]$ with $\Pr[\Delta^i \wedge \neg\Delta^{>i}] > 0$ that*

$$\Pr\left[\Sigma \;\middle|\; \Delta^i \wedge \neg\Delta^{>i}\right] \leq (i-1)\cdot\frac{\bar{L}}{|\mathcal{Y}|} + \frac{1}{|\mathcal{Y}|} \leq \frac{\bar{B}\bar{L}}{|\mathcal{Y}|}\;,$$

where $\bar{L} := q_{\mathcal{D}} + \bar{B} + q_{\mathcal{B}} + \bar{B}$.

The proof is identical to that in Section 4.7.2.

Towards controlling $\Pr[\Sigma \wedge \mathsf{GD} \wedge \Delta'_k]$, the obstacle is that $\mathcal{D}$'s output m may potentially depend on $H(m'_i, z'_i)$, since it has made a hash query to (m'_i, z'_i) and can thus make its output dependent on the hash (e.g., by choosing $m'_{i+1} := H(m'_i, z'_i)$ then). However, by our "sandwich structure" of the hash computation, this is actually not possible. Indeed, since z'_i is a point in *the second part of* the hash chain, all the points in the first part of the chain, i.e., $z_2 := H(m_1, IV)$, $z_3 := H(m_2, z_2)$ up to $z_{B'_1+1} := H(m_{B'_1}, z_{B''})$, must be determined already, and hence all of m as well, *before* $\mathcal{D}$ learns the hash of (m'_i, z'_i).
We bound the probability in the following claim:

Claim 4.36. $\Pr[\Sigma \wedge \mathsf{GD} \wedge \Delta'_k] \leq q_{\mathcal{D}} \cdot r \cdot \bar{B}\bar{L}/|\mathcal{Y}|$.

Proof. Formally, for a fixed choice of k, we consider the following procedure to (try to) extract m from the first k queries made by $\mathcal{D}$ and the replies to the first $k-1$ of these queries: Start with the kth query τ_k and look for a query within $\{\tau_1, \ldots, \tau_{k-1}\}$ that hashes into $\mathsf{R}(\tau_k)$, and then continuing iteratively with that query, until no further such query exists. By construction, this procedure finds $n \leq k$ and $j_1 < \ldots < j_n = k$ such that

$$H(\tau_{j_1}) = \mathsf{R}(\tau_{j_2})\,,\; H(\tau_{j_2}) = \mathsf{R}(\tau_{j_3}), \ldots, H(\tau_{j_{n-1}}) = \mathsf{R}(\tau_{j_n})\,.$$

The procedure then guesses a value $B^\circ \leftarrow [q_{\mathcal{D}}]$ for the number of message blocks and $\ell \leftarrow [r]$ for the exact end of the message within the last message block $m_{B_\circ}$.

The output of the procedure is then defined to be $\hat{m} := (\mathsf{L}(\tau_{j_1}), \ldots, \mathsf{L}(\tau_{j_{B^\circ}}))[1 \ldots \ell]$ where $[1 \ldots \ell]$ refers to the first ℓ bits of the block. First, we observe that $\Sigma \wedge \Gamma \wedge \Delta'_k$ imply that m is a prefix of $(\mathsf{L}(\tau_{j_1}) \| \ldots \| \mathsf{L}(\tau_{j_n}))$, and thus, as $n \leq q_{\mathcal{D}}$, it holds that $\Pr[m = \hat{m} | \Sigma \wedge \Gamma \wedge \Delta'_k] \geq \frac{1}{r \cdot q_{\mathcal{D}}}$.

Indeed, Δ'_k implies that $\tau_k = (m'_i, z'_i)$ for some i, and so

$$\begin{aligned}\mathsf{R}(\tau_k) = z'_i = \mathsf{MD}^H_\perp(m_1 \| \ldots \| m_B \| \mathsf{pk}' \| m'_1 \| \ldots \| m'_{i-1}) \\ = H(m'_{i-1}, z'_{i-1}) = H(\tau_{q_{\mathcal{D}}+q_{\mathcal{B}}+B+i+1})\,.\end{aligned}$$

Hence, by Γ_2, there exists $j_{n-1} < k$ so that $\tau_{j_{n-1}} = \tau_{q_{\mathcal{D}}+B_{\mathsf{pk}}+q_{\mathcal{B}}+i+1} = (m'_{i-1}, z'_{i-1})$, and thus $H(\tau_{j_{n-1}}) = \mathsf{R}(\tau_k)$. Furthermore,

$$\mathsf{R}(\tau_{j_{n-1}}) = z'_{i-1} = \mathsf{MD}^H_\perp(m_1 \| \ldots \| m_B \| \mathsf{pk}' \| m'_1 \| \ldots \| m'_{i-2})\,,$$

and so by repeating the argument, the procedure extracts, in this reversed order, $m'_i, m'_{i-1}, \ldots, m'_1$, some blocks of pk' and $m_{B''_1}, \ldots, m_1$, until $\tau_{j_1} = (m_1, \mathsf{IV})$, which is when the procedure stops (by Γ_3). This allows us to compute the following probability of extracting the correct message:

$$\begin{aligned}\Pr[\Sigma \wedge \mathsf{GD} \wedge \Delta'_k \wedge \hat{m} = m] &= \Pr[\Sigma \wedge \mathsf{GD} \wedge \Delta'_k] \cdot \Pr[m = \hat{m} | \Sigma \wedge \Gamma \wedge \Delta'_k] \\ &\geq \Pr[\Sigma \wedge \mathsf{GD} \wedge \Delta'_k] \cdot \frac{1}{r \cdot q_{\mathcal{D}}}\end{aligned}$$

Now we make the following "game hop", by replacing the experiment

$$\begin{aligned}(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}, \quad m \leftarrow \mathcal{D}^H(\mathsf{sk}), \\ (\mathsf{pk}', y') \leftarrow \mathcal{B}^H\big(\mathsf{sk}, \mathsf{MD}^H(m \| \mathsf{pk} \| m), \mathsf{aux}(\mathsf{sk}, m)\big),\end{aligned}$$

which defined all the above random variables and probabilities, by

$$\begin{aligned}(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}, \quad \hat{m} \leftarrow \hat{\mathcal{D}}^H(\mathsf{sk}), \\ (\mathsf{pk}', y') \leftarrow \mathcal{B}^H\big(\mathsf{sk}, \mathsf{MD}^H(\hat{m} \| \mathsf{pk} \| \hat{m}), \mathsf{aux}(\mathsf{sk}, \hat{m})\big),\end{aligned}$$

where $\hat{\mathcal{D}}$ runs $\mathcal{D}$, but then stops before sending the kth query to H and instead tries to extract m by means of the above procedure from the prior queries. Correspondingly, we denote its output by $\hat{m}$. We stress that $\hat{\mathcal{D}}$ has now query complexity $q_{\hat{\mathcal{D}}} = k - 1$. The crucial observation is that

$$\Pr[\Sigma \wedge \Gamma \wedge \Delta'_k \wedge \hat{m} = m] \leq \widehat{\Pr}[\Sigma \wedge \Delta]$$

Indeed, in case $\hat{m} = m$ there is no difference in the new experiment, except that now $\hat{\mathcal{D}}$ stops before doing the kth query, and so if $\Gamma \wedge \Delta'_k$ is satisfied in the original experiment then Δ is satisfied in the new one. Thus, we can recycle the bound from above. Using the bound $\widehat{\Pr}[\Sigma \wedge \Delta] \leq \bar{B}\bar{L}/|\mathcal{Y}|$ from Claim 4.35 we obtain using the above that

$$\begin{aligned} & \Pr[\Sigma \wedge \mathsf{GD} \wedge \Delta'_k] \cdot \frac{1}{q_{\mathcal{D}} \cdot r} \leq \Pr[\Sigma \wedge \Gamma \wedge \Delta'_k \wedge \hat{m} = m] \\ \Rightarrow \quad & \Pr[\Sigma \wedge \mathsf{GD} \wedge \Delta'_k] \leq q_{\mathcal{D}} \cdot r \cdot \bar{B}\bar{L}/|\mathcal{Y}| \end{aligned}$$

□

We wrap up the proof by adding up the probabilities

$$\begin{aligned} \Pr[\Sigma] &\leq \Pr[\Sigma \wedge \Delta] + \sum_{k=1}^{q_{\mathcal{D}}} \Pr[\Sigma \wedge \Gamma \wedge \Delta'_k] + \Pr[\Sigma \wedge \Gamma \wedge \neg\Lambda] + \Pr[\neg\Gamma] \\ &\leq \frac{\bar{B}\bar{L}}{|\mathcal{Y}|} + \frac{q_{\mathcal{D}}^2 \cdot r \cdot \bar{B}\bar{L}}{|\mathcal{Y}|} + q_{\mathcal{B}} \cdot 2r^2 \cdot \mathbf{Adv}^{\mathsf{HnS}^H}_{\mathsf{MD}_\perp}(\bar{\mathcal{D}}, \bar{\mathcal{A}}) + \frac{q_{\mathcal{D}} + 2\bar{L}^2}{|\mathcal{Y}|} \\ &= q_{\mathcal{B}} \cdot 2r^2 \cdot \mathbf{Adv}^{\mathsf{HnS}^H}_{\mathsf{MD}_\perp}(\bar{\mathcal{D}}, \bar{\mathcal{A}}) + \frac{(q_{\mathcal{D}}^2 \cdot r + 1) \cdot \bar{B}\bar{L} + q_{\mathcal{D}} + 2\bar{L}^2}{|\mathcal{Y}|} \,. \end{aligned}$$

□

Bibliography

[AAB+22] Carlos Aguilar-Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor, Jurjen Bos, Arnaud Dion, Jerome Lacan, Jean-Marc Robert, and Pascal Veron. HQC. Technical report, National Institute of Standards and Technology, 2022. available at `https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions`.

[ABB+17] Erdem Alkim, Nina Bindel, Johannes A. Buchmann, Özgür Dagdelen, Edward Eaton, Gus Gutoski, Juliane Krämer, and Filip Pawlega. Revisiting TESLA in the quantum random oracle model. In Tanja Lange and Tsuyoshi Takagi, editors, *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017*, pages 143–162. Springer, Cham, 2017.

[ABB+20] Erdem Alkim, Paulo S. L. M. Barreto, Nina Bindel, Juliane Krämer, Patrick Longa, and Jefferson E. Ricardini. The lattice-based digital signature scheme qTESLA. In Mauro Conti, Jianying Zhou, Emiliano Casalicchio, and Angelo Spognardi, editors, *ACNS 2020, Part I*, volume 12146 of *LNCS*, pages 441–460. Springer, Cham, October 2020.

[ABK25] Gorjan Alagic, Fahran Bajaj, and Aybars Kocoglu. The best of both KEMs: Securely combining KEMs in post-quantum hybrid schemes. Cryptology ePrint Archive, Paper 2025/1444, 2025.

[ABKM22] Gorjan Alagic, Chen Bai, Jonathan Katz, and Christian Majenz. Post-quantum security of the Even-Mansour cipher. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 458–487. Springer, Cham, May / June 2022.

[AHU19] Andris Ambainis, Mike Hamburg, and Dominique Unruh. Quantum security proofs using semi-classical oracles. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019,*

Part II, volume 11693 of *LNCS*, pages 269–295. Springer, Cham, August 2019.

[Ajt96] Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In *28th ACM STOC*, pages 99–108. ACM Press, May 1996.

[ANSS22] Agence Nationale de la Sécurité des Systémes d'Information (ANSSI). ANSSI views on the post-quantum cryptography transition, 2022. available at `https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition`.

[ARU14] Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *55th FOCS*, pages 474–483. IEEE Computer Society Press, October 2014.

[Bar01] Boaz Barak. How to go beyond the black-box simulation barrier. In *42nd FOCS*, pages 106–115. IEEE Computer Society Press, October 2001.

[BBD+23] Manuel Barbosa, Gilles Barthe, Christian Doczkal, Jelle Don, Serge Fehr, Benjamin Grégoire, Yu-Hsuan Huang, Andreas Hülsing, Yi Lee, and Xiaodi Wu. Fixing and mechanizing the security proof of Fiat-Shamir with aborts and Dilithium. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part V*, volume 14085 of *LNCS*, pages 358–389. Springer, Cham, August 2023.

[BBD+24] Joppe W. Bos, Olivier Bronchain, Léo Ducas, Serge Fehr, Yu-Hsuan Huang, Thomas Pornin, Eamonn W. Postlethwaite, Thomas Prest, Ludo N. Pulles, and Wessel van Woerden. HAWK. Technical report, National Institute of Standards and Technology, 2024. available at `https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures`.

[BBF+19] Nina Bindel, Jacqueline Brendel, Marc Fischlin, Brian Goncalves, and Douglas Stebila. Hybrid key encapsulation mechanisms and authenticated key exchange. In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019*, pages 206–226. Springer, Cham, 2019.

[BCD+24] Manuel Barbosa, Deirdre Connolly, João Diogo Duarte, Aaron Kaiser, Peter Schwabe, Karolin Varner, and Bas Westerbaan. X-wing. *IACR Communications in Cryptology*, 1(1), 2024.

[BCFW09] Alexandra Boldyreva, David Cash, Marc Fischlin, and Bogdan Warinschi. Foundations of non-malleable hash and one-way functions. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 524–541. Springer, Berlin, Heidelberg, December 2009.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 41–69. Springer, Berlin, Heidelberg, December 2011.

[BDK+22] Ward Beullens, Samuel Dobson, Shuichi Katsumata, Yi-Fu Lai, and Federico Pintore. Group signatures and more from isogenies and lattices: Generic, simple, and efficient. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 95–126. Springer, 2022.

[BDPA07] G.M. Bertoni, Joan Daemen, Michael Peeters, and Gilles Assche. Sponge functions. *ECRYPT Hash Workshop 2007*, 01 2007.

[Beu21] Ward Beullens. Mayo: Practical post-quantum signatures from oil-and-vinegar maps. In *Selected Areas in Cryptography: 28th International Conference*, 2021.

[BFS11] Paul Baecher, Marc Fischlin, and Dominique Schröder. Expedient non-malleability notions for hash functions. In Aggelos Kiayias, editor, *CT-RSA 2011*, volume 6558 of *LNCS*, pages 268–283. Springer, Berlin, Heidelberg, February 2011.

[BG81] Charles H. Bennett and John Gill. Relative to a random oracle A, $\mathbf{P}^A \neq \mathbf{NP}^A \neq \text{co-}\mathbf{NP}^A$ with probability 1. *SIAM Journal on Computing*, 10(1):96–113, 1981.

[BKP20] Ward Beullens, Shuichi Katsumata, and Federico Pintore. Calamari and Falafl: logarithmic (linkable) ring signatures from isogenies and lattices. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 464–492. Springer, 2020.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM CCS 93*, pages 62–73. ACM Press, November 1993.

[BV93] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. In *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing*, pages 11–20, 1993.

[CAD+24] Alessandro Chiesa, Marcel Dall Agnol, Zijing Di, Ziyi Guan, and Nicholas Spooner. Quantum rewinding for iop-based succinct arguments, 2024.

[CCD+24] Jung Hee Cheon, Hyeongmin Choe, Julien Devevey, Tim Güneysu, Dongyeon Hong, Markus Krausz, Georg Land, Marc Möller, Damien Stehlé, and MinJune Yi. Haetae: Shorter lattice-based Fiat-Shamir signatures. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2024, 2024.

[CD20] André Chailloux and Thomas Debris-Alazard. Tight and optimal reductions for signatures based on average trapdoor preimage sampleable functions and applications to code-based signatures. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part II*, volume 12111 of *LNCS*, pages 453–479. Springer, Cham, May 2020.

[CDF+21] Cas Cremers, Samed Düzlü, Rune Fiedler, Marc Fischlin, and Christian Janson. BUFFing signature schemes beyond unforgeability and the case of post-quantum signatures. In *2021 IEEE Symposium on Security and Privacy*, pages 1696–1714. IEEE Computer Society Press, May 2021.

[CDF+23] Cas Cremers, Samed Düzlü, Rune Fiedler, Marc Fischlin, and Christian Janson. BUFFing signature schemes beyond unforgeability and the case of post-quantum signatures, 2023. An updated version (Version 1.4) of [CDF+21], available at `https://eprint.iacr.org/archive/2020/1525/20231020:082812`.

[CDP23] Sanjit Chatterjee, M. Prem Laxman Das, and Tapas Pandit. Revisiting the security of salted uov signature. In *Progress in Cryptology – INDOCRYPT 2022*, 2023.

[CFHL21] Kai-Min Chung, Serge Fehr, Yu-Hsuan Huang, and Tai-Ning Liao. On the compressed-oracle technique, and post-quantum security of proofs of sequential work. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 598–629. Springer, Cham, October 2021.

[CFMR+17] Antoine Casanova, Jean-Charles Faugère, Gilles Macario-Rat, Jacques Patarin, Ludovic Perret, and Jocelyn Ryckeghem. GeMSS: A Great Multivariate Short Signature. Research report, December 2017.

[CFS01] Nicolas T. Courtois, Matthieu Finiasz, and Nicolas Sendrier. How to achieve a McEliece-based digital signature scheme. In Colin Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*, 2001.

[CGH04] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. *J. ACM*, 51(4):557–594, July 2004.

[CGLQ20] Kai-Min Chung, Siyao Guo, Qipeng Liu, and Luowen Qian. Tight quantum time-space tradeoffs for function inversion. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 673–684, 2020.

[CHH+21] Kai-Min Chung, Yao-Ching Hsieh, Mi-Ying Huang, Yu-Hsuan Huang, Tanja Lange, and Bo-Yin Yang. Isogeny-based group signatures and accountable ring signatures in QROM. Cryptology ePrint Archive, Paper 2021/1368, 2021.

[CMSZ22] Alessandro Chiesa, Fermi Ma, Nicholas Spooner, and Mark Zhandry. Post-quantum succinct arguments: Breaking the quantum rewinding barrier. In *62nd FOCS*, pages 49–58. IEEE Computer Society Press, February 2022.

[Cou06] Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006.

[Dal08] Léonard Dallot. Towards a concrete security proof of courtois, finiasz and sendrier signature scheme. In *Research in Cryptology*, 2008.

[Dam90] Ivan Damgård. A design principle for hash functions. In Gilles Brassard, editor, *CRYPTO'89*, volume 435 of *LNCS*, pages 416–427. Springer, New York, August 1990.

[dEK+23] Rafael del Pino, Thomas Espitau, Shuichi Katsumata, Mary Maller, Fabrice Mouhartem, Thomas Prest, Mélissa Rossi, and Markku-Juhani Saarinen. Raccoon. Technical report, National Institute of Standards and Technology, 2023. available at `https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures`.

[Deu85] David Deutsch. Quantum theory, the church–turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

[DFG13] Özgür Dagdelen, Marc Fischlin, and Tommaso Gagliardoni. The Fiat-Shamir transformation in a quantum world. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part II*, volume 8270 of *LNCS*, pages 62–81. Springer, Berlin, Heidelberg, December 2013.

[DFG19a] Luca De Feo and Steven D. Galbraith. Seasign: Compact isogeny signatures from class group actions. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, 2019.

[DFG19b] Luca De Feo and Steven D Galbraith. SeaSign: compact isogeny signatures from class group actions. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 759–789. Springer, 2019.

[DFH22] Jelle Don, Serge Fehr, and Yu-Hsuan Huang. Adaptive versus static multi-oracle algorithms, and quantum security of a split-key PRF. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 33–51. Springer, Cham, November 2022.

[DFH+24] Jelle Don, Serge Fehr, Yu-Hsuan Huang, Jyun-Jie Liao, and Patrick Struck. Hide-and-seek and the non-resignability of the BUFF transform. In Elette Boyle and Mohammad Mahmoody, editors, *TCC 2024, Part III*, volume 15366 of *LNCS*, pages 347–370. Springer, Cham, December 2024.

[DFHS24] Jelle Don, Serge Fehr, Yu-Hsuan Huang, and Patrick Struck. On the (in)security of the BUFF transform. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part I*, volume 14920 of *LNCS*, pages 246–275. Springer, Cham, August 2024.

[DFM20] Jelle Don, Serge Fehr, and Christian Majenz. The measure-and-reprogram technique 2.0: Multi-round fiat-shamir and more. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part III*, volume 12172 of *LNCS*, pages 602–631. Springer, Cham, August 2020.

[DFMS19] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Security of the Fiat-Shamir transformation in the quantum random-oracle model. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 356–383. Springer, Cham, August 2019.

[DFPS23] Julien Devevey, Pouria Fallahpour, Alain Passelègue, and Damien Stehlé. A detailed analysis of Fiat-Shamir with aborts. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part V*, volume 14085 of *LNCS*, pages 327–357. Springer, Cham, August 2023.

[DG19] Luca De Feo and Steven D. Galbraith. SeaSign: Compact isogeny signatures from class group actions. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part III*, volume 11478 of *LNCS*, pages 759–789. Springer, Cham, May 2019.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[DKL+18] Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018.

[DS23] Marcel Dall'Agnol and Nicholas Spooner. On the necessity of collapsing for post-quantum and quantum commitments. In *18th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2023)*, volume 266 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 2:1–2:23, Dagstuhl, Germany, July 2023. Schloss Dagstuhl - Leibniz-Zentrum für Informatik.

[DST19] Thomas Debris-Alazard, Nicolas Sendrier, and Jean-Pierre Tillich. Wave: A new family of trapdoor one-way preimage sampleable functions based on codes. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019*, 2019.

[EHH+22] S Ehlen, H Hagemeier, T Hemmert, S Kousidis, M Lochter, S Reinhardt, and T Wunderer. Quantum-safe cryptography–fundamentals, current developments and recommendation. *Federal Office for Information Security (BSI), Godesberger Allee*, pages 185–189, 2022.

[ENST23] Thomas Espitau, Guilhem Niot, Chao Sun, and Mehdi Tibouchi. SQUIRRELS — Square Unstructured Integer Euclidean Lattice Signature. Technical report, National Institute of Standards and Technology, 2023. available at `https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures`.

[FFH25] Pouria Fallahpour, Serge Fehr, and Yu-Hsuan Huang. Tighter quantum security for Fiat-Shamir-with-aborts and hash-and-sign-with-retry signatures. Cryptology ePrint Archive, Paper 2025/985, 2025.

[FH23] Serge Fehr and Yu-Hsuan Huang. On the quantum security of HAWK. In Thomas Johansson and Daniel Smith-Tone, editors, *Post-Quantum Cryptography - 14th International Workshop, PQCrypto 2023*, pages 405–416. Springer, Cham, August 2023.

[FHA23] Serge Fehr, Yu-Hsuan Huang, and Alessandro Amadori. Literature review - (quantum-safe) cryptographic combiners and hybrid security. Technical report, 2023. available at `https://hapkido.tno.nl/deliverables/literature-review-quantum-safe/`.

[FHK+22] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon - whats next? `https://csrc.nist.gov/csrc/media/Presentations/2022/falcon-update/images-media/session-1-prest-falcon-pqc2022.pdf`, 2022.

[FHK25] Serge Fehr, Yu-Hsuan Huang, and Julia Kastner. Sandwich BUFF: Achieving non-resignability using iterative hash functions. In Benny Applebaum and Huijia (Rachel) Lin, editors, *TCC 2025, Part III*, volume 16270 of *LNCS*, pages 235–265. Springer, Cham, December 2025.

[FIKT21] Hiroki Furue, Yasuhiko Ikematsu, Yutaro Kiyomura, and Tsuyoshi Takagi. A new variant of unbalanced oil and vinegar using quotient ring: Qr-uov. In *Advances in Cryptology – ASIACRYPT 2021*, 2021.

[FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 537–554. Springer, Berlin, Heidelberg, August 1999.

[FO13] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. *Journal of Cryptology*, 26(1):80–101, January 2013.

[FS87] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *CRYPTO'86*, volume 263 of *LNCS*, pages 186–194. Springer, Berlin, Heidelberg, August 1987.

[GCF+23] Louis Goubin, Benoît Cogliati, Jean-Charles Faugère, Pierre-Alain Fouque, Robin Larrieu, Gilles Macario-Rat, Brice Minaud, and Jacques Patarin. PROV — PRovable unbalanced Oil and Vinegar. Technical report, National Institute of Standards and Technology, 2023. available at `https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures`.

[GHHM21] Alex B. Grilo, Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz. Tight adaptive reprogramming in the QROM. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part I*, volume 13090 of *LNCS*, pages 637–667. Springer, Cham, December 2021.

[GHP18] Federico Giacon, Felix Heuer, and Bertram Poettering. KEM combiners. In Michel Abdalla and Ricardo Dahab, editors, *PKC 2018, Part I*, volume 10769 of *LNCS*, pages 190–218. Springer, Cham, March 2018.

[GJK24] Phillip Gajland, Jonas Janneck, and Eike Kiltz. A closer look at falcon. *Cryptology ePrint Archive*, 2024.

[GK03] Shafi Goldwasser and Yael Tauman Kalai. On the (in)security of the Fiat-Shamir paradigm. In *44th FOCS*, pages 102–115. IEEE Computer Society Press, October 2003.

[GL89] Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In *21st ACM STOC*, pages 25–32. ACM Press, May 1989.

[GLP12] Tim Güneysu, Vadim Lyubashevsky, and Thomas Pöppelmann. Practical lattice-based cryptography: A signature scheme for embedded systems. In *Workshop on Cryptographic Hardware and Embedded Systems*, 2012.

[GM82] Shafi Goldwasser and Silvio Micali. Probabilistic encryption and how to play mental poker keeping secret all partial information. In *14th ACM STOC*, pages 365–377. ACM Press, May 1982.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008.

[HBD+20] Andreas Hülsing, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger,

Joost Rijneveld, Peter Schwabe, Jean-Philippe Aumasson, Bas Westerbaan, and Ward Beullens. SPHINCS$^+$. Technical report, National Institute of Standards and Technology, 2020. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions`.

[HBD+22] Andreas Hülsing, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, Jean-Philippe Aumasson, Bas Westerbaan, and Ward Beullens. SPHINCS$^+$. Technical report, National Institute of Standards and Technology, 2022. available at `https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022`.

[HC18] Yu-Hsuan Huang and Rong-Jaye Chen. Simulating quantum algorithm by using singular value decomposition. In *Cryptology and Information Security Conference*, 2018.

[HV21] Loïs Huguenin-Dumittan and Serge Vaudenay. FO-like combiners and hybrid post-quantum cryptography. In Mauro Conti, Marc Stevens, and Stephan Krenn, editors, *CANS 21*, volume 13099 of *LNCS*, pages 225–244. Springer, Cham, December 2021.

[HYC20] Yu-Hsuan Huang, Chih-Kai Yang, and Rong-Jaye Chen. Quadrangle inequality improvement for CSIDH strategy. In *Cryptology and Information Security Conference*, 2020.

[IR90] Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In Shafi Goldwasser, editor, *CRYPTO'88*, volume 403 of *LNCS*, pages 8–26. Springer, New York, August 1990.

[JCCS19] Dennis Jackson, Cas Cremers, Katriel Cohn-Gordon, and Ralf Sasse. Seems legit: Automated analysis of subtle attacks on protocols that use signatures. In Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang, and Jonathan Katz, editors, *ACM CCS 2019*, pages 2165–2180. ACM Press, November 2019.

[JST21] Joseph Jaeger, Fang Song, and Stefano Tessaro. Quantum key-length extension. In Kobbi Nissim and Brent Waters, editors, *TCC 2021, Part I*, volume 13042 of *LNCS*, pages 209–239. Springer, Cham, November 2021.

[KBJ+14] Tiffany Hyun-Jin Kim, Cristina Basescu, Limin Jia, Soo Bum Lee, Yih-Chun Hu, and Adrian Perrig. Lightweight source authentication and path validation. In *Proceedings of the 2014 ACM Conference on SIGCOMM*, pages 271–282, 2014.

[KLS18] Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 552–586. Springer, Cham, April / May 2018.

[KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In *Advances in Cryptology — EUROCRYPT '99*, 1999.

[KRS25] Dmitry Khovratovich, Ron D. Rothblum, and Lev Soukhanov. How to prove false statements: Practical attacks on fiat-shamir. Cryptology ePrint Archive, Paper 2025/118, 2025.

[KX24] Haruhisa Kosuge and Keita Xagawa. Probabilistic hash-and-sign with retry in the quantum random oracle model. In Qiang Tang and Vanessa Teague, editors, *PKC 2024, Part I*, volume 14601 of *LNCS*, pages 259–288. Springer, Cham, April 2024.

[Lam79] Leslie Lamport. Constructing digital signatures from a one-way function. Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, October 1979.

[LDK+20] Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehlé, and Shi Bai. CRYSTALS-DILITHIUM. Technical report, National Institute of Standards and Technology, 2020. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions`.

[LDK+22] Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehlé, and Shi Bai. CRYSTALS-DILITHIUM. Technical report, National Institute of Standards and Technology, 2022. available at `https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022`.

[LMS22] Russell W. F. Lai, Giulio Malavolta, and Nicholas Spooner. Quantum rewinding for many-round protocols. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 80–109. Springer, Cham, November 2022.

[LNP22] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Maxime Plancon. Lattice-based zero-knowledge proofs and applications: Shorter, simpler, and more general. *Cryptology ePrint Archive*, 2022.

[LS19] Vadim Lyubashevsky and Peter Schwabe. Round 2 official comment: qTESLA. `https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/official-comments/qTESLA-round2-official-comment.pdf`, 2019. Accessed: 18-05-2022.

[Lyu09] Vadim Lyubashevsky. Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. In Mitsuru Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, 2009.

[Lyu12] Vadim Lyubashevsky. Lattice signatures without trapdoors. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, 2012.

[LZ19] Qipeng Liu and Mark Zhandry. Revisiting post-quantum Fiat-Shamir. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 326–355. Springer, Cham, August 2019.

[LZ23] Dongxi Liu and Raymond K. Zhao. eMLE-Sig 2.0 — Embedded Multilayer Equations with Heavy Layer Randomization. Technical report, National Institute of Standards and Technology, 2023. available at `https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures`.

[McE78] Robert J. McEliece. A public-key cryptosystem based on algebraic coding theory. The deep space network progress report 42-44, Jet Propulsion Laboratory, California Institute of Technology, January/February 1978. `https://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF`.

[Mer79] Ralph Charles Merkle. *Secrecy, authentication, and public key systems.* PhD thesis, Stanford University, Stanford, CA, USA, 1979. AAI8001972.

[Mer90] Ralph C. Merkle. One way hash functions and DES. In Gilles Brassard, editor, *CRYPTO'89*, volume 435 of *LNCS*, pages 428–446. Springer, New York, August 1990.

[MI88] Tsutomu Matsumoto and Hideki Imai. Public quadratic polynominal-tuples for efficient signature-verification and message-encryption. In C. G. Günther, editor, *EUROCRYPT'88*,

volume 330 of *LNCS*, pages 419–453. Springer, Berlin, Heidelberg, May 1988.

[NIST22] National Institute of Standards and Technology. Call for additional digital signature schemes for the post-quantum cryptography standardization process. `https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf`, 2022.

[NSA24] National Security Agency (NSA). The commercial national security algorithm suite 2.0 and quantum computing FAQ, 2024. available at `https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF`.

[Pat96] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In Ueli Maurer, editor, *Advances in Cryptology — EUROCRYPT '96*, 1996.

[PCF+23] Jacques Patarin, Benoît Cogliati, Jean-Charles Faugère, Pierre-Alain Fouque, Louis Goubin, Robin Larrieu, Gilles Macario-Rat, and Brice Minaud. VOX. Technical report, National Institute of Standards and Technology, 2023. available at `https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures`.

[PFH+20] Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. FALCON. Technical report, National Institute of Standards and Technology, 2020. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions`.

[PFH+22] Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. FALCON. Technical report, National Institute of Standards and Technology, 2022. available at `https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022`.

[PS96] David Pointcheval and Jacques Stern. Security proofs for signature schemes. In Ueli M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 387–398. Springer, Berlin, Heidelberg, May 1996.

[PS05] Thomas Pornin and Julien P. Stern. Digital signatures do not guarantee exclusive ownership. In John Ioannidis, Angelos Keromytis, and Moti Yung, editors, *ACNS 2005*, volume 3531 of *LNCS*, pages 138–150. Springer, Berlin, Heidelberg, June 2005.

[RSS11] Thomas Ristenpart, Hovav Shacham, and Thomas Shrimpton. Careful with composition: Limitations of the indifferentiability framework. In Kenneth G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 487–506. Springer, Berlin, Heidelberg, May 2011.

[SAB+22] Peter Schwabe, Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, Damien Stehlé, and Jintai Ding. CRYSTALS-KYBER. Technical report, National Institute of Standards and Technology, 2022. available at `https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022`.

[SFG25] Douglas Stebila, Scott Fluhrer, and Shay Gueron. Hybrid key exchange in TLS 1.3. Internet-Draft draft-ietf-tls-hybrid-design-15, Internet Engineering Task Force, September 2025. Work in Progress.

[Sha49] Claude E. Shannon. Communication theory of secrecy systems. *Bell Systems Technical Journal*, 28(4):656–715, 1949.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th FOCS*, pages 124–134. IEEE Computer Society Press, November 1994.

[Sim94] D.R. Simon. On the power of quantum computation. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 116–123, 1994.

[SSH11] Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari. On provable security of UOV and HFE signature schemes against chosen-message attack. In *Post-Quantum Cryptography*, 2011.

[TTB+23] C. Tjhai, M. Tomlinson, G. Bartlett, Scott Fluhrer, Daniel Van Geest, Oscar Garcia-Morchon, and Valery Smyslov. Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2). RFC 9370, May 2023.

[Unr12] Dominique Unruh. Quantum proofs of knowledge. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 135–152. Springer, Berlin, Heidelberg, April 2012.

[Unr15] Dominique Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 755–784. Springer, Berlin, Heidelberg, April 2015.

[Unr16] Dominique Unruh. Computationally binding quantum commitments. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 497–527. Springer, Berlin, Heidelberg, May 2016.

[Unr17] Dominique Unruh. Post-quantum security of Fiat-Shamir. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 65–95. Springer, Cham, December 2017.

[Wil11] Mark M Wilde. From classical to quantum Shannon theory. *arXiv preprint arXiv:1106.1445*, 2011.

[ZBPB17] Jean Karim Zinzindohoué, Karthikeyan Bhargavan, Jonathan Protzenko, and Benjamin Beurdouche. HACL*: A verified modern cryptographic library. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS 2017*, pages 1789–1806. ACM Press, October / November 2017.

[Zha12] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, Berlin, Heidelberg, August 2012.

[Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 239–268. Springer, Cham, August 2019.