AICR · OPEN PROBLEM

Simultaneous Inversion of a One-Way Function and a Random Permutation Given a Collision Finder

The strong amplification conjecture behind Simon's oracle

Status. Statement: AI-written from Geoffroy Couteau, Pooya Farshim and Mohammad Mahmoody, *Black-Box Uselessness: Composing Separations in Cryptography*, Cryptology ePrint Archive 2021, not yet checked by a human. Open in the stated generality. The paper's weak version without the collision finder (Conjecture 6.6) is known when the one-way function is itself a random oracle, but not for an arbitrary one-way function; the strong version with the collision finder is not claimed to be known in any case. The pure random-permutation inversion bound without a second function is classical [IR89], and survives the collision finder [Sim98].

Category. *Black-Box Separations & Reductions.*

Conjecture (informal). *Take any function that is hard to invert, in the sense that no efficient adversary inverts a random image with probability better than some bound. Independently, take a uniformly random permutation on strings of the same length; inverting that has probability at most polynomially more than one over the size of the domain, and this remains true even for an adversary handed an oracle that, given any circuit built out of permutation gates and recursive collision-finder gates, returns a uniformly random collision for it. The conjecture is that these two hardnesses multiply: an adversary given an image under the hard function and an image under the permutation, and with access to the function, the permutation and the collision finder, cannot output both preimages with probability better than the product of the two bounds, up to a polynomial factor. The paper's weaker version of this statement — the same product bound but without the collision finder present (Conjecture 6.6) — is known when the hard function is itself a random oracle, but not when it is an arbitrary one-way function. The strong version stated here, with the collision finder, is not claimed to be known in any case. The paper needs it to conclude that adding a one-way function to the permutation-plus-collision-finder pair yields a pair of functions that is hard to invert simultaneously, which by a known construction gives collision-resistant hashing, and therefore that one-way functions are helpful for collision resistance even though they cannot produce it alone.*

1 The setting

Impagliazzo and Rudich [IR89] showed that for any attacker, with measure one over the choice of a random permutation RP, the permutation cannot be inverted with probability better than $\mathrm{poly}(\lambda)/2^{\lambda}$. Simon [Sim98] showed that this survives the presence of a collision finder $\mathsf{Coll}^{\mathsf{RP}}$ that returns a random collision for any oracle circuit with RP-gates and recursive Coll-gates; since Coll trivially breaks collision resistance, this is exactly what separates collision-resistant hashing from one-way permutations. Both statements extend to a setting where an auxiliary oracle independent of $(\mathsf{RP}, \mathsf{Coll})$ is present.

The conjecture asks for a *product* version of these facts. Holmgren

and Lombardi [HL18] showed that exponentially secure one-way product functions, that is, tuples of functions whose images cannot all be inverted simultaneously with probability better than roughly $2^{-\lambda}$, black-box imply collision-resistant hash functions. The present paper's route to showing that one-way functions are black-box helpful for collision resistance is to take the auxiliary primitive to be Simon's pair $(\pi, \mathsf{Coll}^{\pi})$ and to argue that for *any* one-way function F the pair $(\mathsf{F}, (\pi, \mathsf{Coll}^{\pi}))$ is product one-way; the intuition offered is that π is fully independent of F, so all an adversary can do is invert the two independently. Formalizing this is precisely the conjecture stated here, and the authors record that they could not prove it and leave it as an open problem of possible independent interest, noting a connection to hardness amplification.

The paper first states a weak version without the collision finder (Conjecture 6.6), remarks that even that is known only when F is itself a random oracle rather than an arbitrary one-way function, and then states the strong version with the collision finder (Conjecture 6.7) as what is actually needed. A footnote in the introduction suggests an easier warm-up: given an ε-secure one-way permutation and a random oracle, can an attacker invert both simultaneously with probability better than $\mathrm{negl}(n)/2^n$? Two theorems make the payoff concrete: the strong version implies both relaxations of the paper's headline helpfulness conjecture, the distributional one and the class-reduction one. The paper also presents a second, unrelated approach via backdoored random oracles [BFM18], whose leakage oracle is powerful enough to implement Simon's collision finder. Under a communication-complexity conjecture related to set intersection, two independent backdoored random oracles yield a collision-resistant hash function, so a single backdoored random oracle — an idealized primitive black-box separated from collision-resistant hash functions — is conjecturally black-box helpful for them. This yields a helpful idealized primitive, not the helpfulness of one-way functions, and does not bear on the conjecture stated here.

Progress to date. The paper states the weak version (no collision finder) as Conjecture 6.6 and records that it is known when the one-way function is a random oracle. Theorem 6.8 shows the strong version implies that one-way functions are distributionally fully black-box helpful for collision-resistant hash functions, and Theorem 6.12

shows it implies the class-helpfulness relaxation. A weaker warm-up is suggested in footnote 9: replace the arbitrary one-way function by an ε-secure one-way permutation and the random permutation with its collision finder by a random oracle, and ask whether an attacker can invert both simultaneously with probability better than $\mathrm{negl}(n)/2^n$.

2 Notation and parameters

- $\lambda \in \mathbb{N}$ is the security parameter; PPT means probabilistic polynomial time; an *oracle-aided PPT* machine runs in polynomial time relative to every oracle, each oracle call counting as one step.
- $\varepsilon : \mathbb{N} \to (0,1]$ is the inversion advantage bound for the one-way function; it is an arbitrary function, not required to be negligible.
- F is an oracle implementing a function on $\{0,1\}^\lambda$ for each λ, fixed before RP is sampled; $\mathsf{F}^{-1}(y)$ is its preimage set.
- $\mathsf{RP} = \{\mathsf{RP}_\lambda\}_\lambda$ is a random permutation: for each λ, RP_λ is a uniformly random permutation of $\{0,1\}^\lambda$, sampled independently across λ. "For a measure one of RP" means with probability 1 over this sampling.
- $\mathsf{Coll}^{\mathsf{RP}}$ is Simon's collision finder for RP (Definition 1); "for a measure one of collision-finders" means with probability 1 over the randomness fixing its answers.
- A is the adversary, with oracle access to F, RP and $\mathsf{Coll}^{\mathsf{RP}}$; poly is a polynomial depending on A.

3 The conjecture

Definition 1 (Simon's collision finder). Let $\mathsf{RP} = \{\mathsf{RP}_\lambda\}_\lambda$ be a permutation oracle. The *collision finder* $\mathsf{Coll}^{\mathsf{RP}}$ is the oracle that, on input a circuit C whose gates are ordinary Boolean gates, RP-gates and (recursively) Coll-gates, samples a uniformly random point x in the domain of C, then samples a

uniformly random x' with $C(x') = C(x)$, and returns (x, x'). Its answers are fixed in advance by independent uniform choices, so that "a measure one of collision-finders $\mathsf{Coll}^{\mathsf{RP}}$" refers to the product measure over these choices.

Definition 2 (ε-secure one-way function). An oracle F *implements an ε-secure one-way function* if no oracle-aided PPT machine B with access to F inverts $\mathsf{F}(x)$ on a uniformly random $x \in \{0,1\}^\lambda$ with probability better than $\varepsilon(\lambda)$, for all sufficiently large λ.

Conjecture 1 (product hardness of F and RP given $\mathsf{Coll}^{\mathsf{RP}}$). *Let $\varepsilon : \mathbb{N} \to (0,1]$ be any function. Let F be any oracle implementing an ε-secure one-way function, that is, for every oracle-aided PPT machine B and all sufficiently large λ,*

$$\Pr_{x \leftarrow \{0,1\}^\lambda} \left[B^{\mathsf{F}}(1^\lambda, \mathsf{F}(x)) \in \mathsf{F}^{-1}(\mathsf{F}(x)) \right] \le \varepsilon(\lambda).$$

Then for every oracle-aided PPT machine A there exists a polynomial poly *such that, for a measure one of random permutations $\mathsf{RP} = \{\mathsf{RP}_\lambda\}_{\lambda \in \mathbb{N}}$ and collision-finders $\mathsf{Coll}^{\mathsf{RP}}$, and for all sufficiently large λ,*

$$\Pr\left[(x_1, x_2) = A^{\mathsf{F},\mathsf{RP},\mathsf{Coll}^{\mathsf{RP}}}\left(\mathsf{F}(x_1), \mathsf{RP}(x_2)\right) \right] \le \varepsilon(\lambda) \cdot \frac{\mathrm{poly}(\lambda)}{2^\lambda},$$

where the probability is taken over the choice of $(x_1, x_2) \leftarrow (\{0,1\}^\lambda)^2$ and over the coins of A.

Remark 1 (a typo repaired in the displayed inequality). The paper writes $\mathsf{P}(x_1)$ here; this is a typo for $\mathsf{F}(x_1)$, as F is the only function in scope and P denotes the implementation machine of a black-box reduction elsewhere in the paper. The same substitution applies to the corresponding display in the weak version, Conjecture 6.6.

Remark 2 (readings fixed by the compositor). Two points are left implicit in the source and have been read in the standard way. First, the quantifier on $\mathrm{poly}(\lambda)$ is taken to be existential and to come after the adversary A, so the polynomial may depend on A. Second, the ε-security of F in Definition 2 is required only against machines with access to F, and not against machines that also query RP and $\mathsf{Coll}^{\mathsf{RP}}$; this is the stronger reading of the conjecture. Note that F must be fixed before RP is sampled for the measure-one quantifier to be meaningful.

4 Bibliography

[BFM18] B. Bauer, P. Farshim, S. Mazaheri. *Combiners for backdoored random oracles.* CRYPTO 2018, Part II, LNCS 10992, pages 272–302, Springer, 2018.

[HL18] J. Holmgren, A. Lombardi. *Cryptographic hashing from strong one-way functions (or: One-way product functions and their applications).* 59th Annual Symposium on Foundations of Computer Science, pages 850–858, IEEE Computer Society Press, 2018.

[IR89] R. Impagliazzo, S. Rudich. *Limits on the provable consequences of one-way permutations.* 21st Annual ACM Symposium on Theory of Computing, pages 44–61, ACM Press, 1989.

[Sim98] D. R. Simon. *Finding collisions on a one-way street: Can secure hash functions be based on general assumptions?* EUROCRYPT'98, LNCS 1403, pages 334–345, Springer, 1998.