Ideal-Cipher (Ir)reducibility for Blockcipher-Based Hash Functions

Paul Baecher[1] Pooya Farshim[1] Marc Fischlin[1] Martijn Stam[2]

[1] Department of Computer Science, Darmstadt University of Technology, Germany
www.cryptoplexity.de
[2] Department of Computer Science, University of Bristol, UK

Abstract. Preneel et al. (Crypto 1993) assessed 64 possible ways to construct a compression function out of a blockcipher. They conjectured that 12 out of these 64 so-called PGV constructions achieve optimal security bounds for collision resistance and preimage resistance. This was proven by Black et al. (Journal of Cryptology, 2010), if one assumes that the blockcipher is ideal. This result, however, does not apply to "non-ideal" blockciphers such as AES. To alleviate this problem, we revisit the PGV constructions in light of the recently proposed idea of random-oracle reducibility (Baecher and Fischlin, Crypto 2011). We say that the blockcipher in one of the 12 secure PGV constructions reduces to the one in another construction, if *any* secure instantiation of the cipher, ideal or not, for one construction also makes the other secure. This notion allows us to relate the underlying assumptions on blockciphers in different constructions, and show that the requirements on the blockcipher for one case are not more demanding than those for the other. It turns out that this approach divides the 12 secure constructions into two groups of equal size, where within each group a blockcipher making one construction secure also makes all others secure. Across the groups this is provably not the case, showing that the sets of "good" blockciphers for each group are qualitatively distinct. We also relate the ideal ciphers in the PGV constructions with those in double-block-length hash functions such as Tandem-DM, Abreast-DM, and Hirose-DM. Here, our results show that, besides achieving better bounds, the double-block-length hash functions rely on weaker assumptions on the blockciphers to achieve collision and everywhere preimage resistance.

1 Introduction

The design of hash functions (or compression functions) from blockciphers has been considered very early in modern cryptography. Preneel, Govaerts, and Vandewalle [PGV94] initiated a systematic study of designing a compression function $\mathsf{F} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ out of a blockcipher $\mathsf{E} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ by analyzing all 64 possible ways to combine the relevant inputs and outputs using xors only. Preneel et al. conjectured only 12 out of these 64 PGV constructions to be secure, including the well-known constructions of Matyas–Meyer–Oseas (MMO) and Davies–Meyer (DM). The idea continues to influence hash-function design till today. Indeed, one of the former five final candidates in the SHA-3 competition, Skein [FLS+08], explicitly refers to this design methodology, and other former candidates like Grøstl [GKM+11] are based on similar principles.

The conjecture about the 12 secure PGV variants was later shown to be true in the *ideal-cipher model* (ICM) by Black et al. [BRS02, BRSS10]. Roughly speaking, Black et al. show that assuming E implements a random blockcipher, the 12 secure PGV compression functions achieve optimal security of $\Theta(q^2 \cdot 2^{-n})$ for collision resistance and $\Theta(q \cdot 2^{-n})$ for preimage resistance, where q is the number of queries to the ideal cipher (and its inverse). Black et al. also discuss 8 further variants which, if used in an iteration mode, attain optimal collision resistance and suboptimal preimage resistance of $\Theta(q^2 \cdot 2^{-n})$. The remaining 44 PGV versions are insecure.

IDEALIZED MODELS. As pointed out by Black et al. [BRSS10], security proofs for the PGV schemes in the ICM should be treated with care. Such results indicate that in order to break the security of the PGV scheme one would need to take advantage of structural properties of the blockcipher. Yet blockciphers such as AES, or the Threefish blockcipher used in Skein, clearly display a structure which is far from an ideal object. For instance, IDEA seems quite unsuitable to base a compression function on [WPS+12], while for AES recent related-key attacks [BK09, BKN09] cast some shadow on its suitability for this purpose. Indeed, Khovratovich [Kho10, Corollary 2] states unambiguously that "AES-256 in the Davies–Meyer hashing mode leads to an insecure hash function," but remarks that it is not known how to attack, for instance, double-block-length constructions. Moreover, it is currently still unknown how to exploit these weaknesses in AES-256 to break the standard collision or preimage security of any AES-instantiated PGV compression function. Consequently it may well be that AES makes some of the 12 PGV constructions secure, whereas others turn out to be insecure, despite a proof in the ICM. Unfortunately, it is very hard to make any security claims about specific PGV constructions with respect to a "real" blockcipher, or to even determine exactly the necessary requirements on the blockcipher for different PGV constructions to be secure.

Recently, a similar issue for the random-oracle model, where a monolithic idealized hash function is used, has been addressed by Baecher and Fischlin [BF11] via the so-called random-oracle reducibility. The idea is to relate the idealized hash functions in different (primarily public-key) schemes, allowing to conclude that the requirements on the hash function in one scheme are weaker than those in the other scheme. That is, Baecher and Fischlin consider two cryptographic schemes A and B with related security games in the random-oracle model. They define that the random oracle in scheme B reduces to the one in scheme A, if *any* instantiation $\mathcal{H}$ of the random oracle, possibly through an efficient hash function or again by an oracle-based solution, which makes scheme A secure, also makes scheme B secure. As such, the requirements on the hash function for scheme B are weaker than those for the one in scheme A. To be precise, Baecher and Fischlin allow an efficient but deterministic and stateless transformation $\mathcal{T}^{\mathcal{H}}$ for instantiating the random oracle in scheme B, to account for, say, different input or output sizes of the hash functions in the schemes. Using such transformations they are able to relate the random oracles in some public-key encryption schemes, including some ElGamal-type schemes.

OUR RESULTS FOR THE PGV CONSTRUCTIONS. We apply the idea of oracle reducibility to the ideal-cipher model and the PGV constructions. Take any two of the 12 PGV constructions, PGV_i and PGV_j, which are secure in the ICM. The goal is to show that any blockcipher (ideal or not) which makes PGV_i secure, also makes PGV_j secure. Here, security may refer to different games such as standard notion for collision resistance, preimage resistance, or everywhere preimage resistance [RS04], or more elaborate notions such as preimage awareness [DRS09]. Although we can ask the same question for indifferentiability from random functions [MRH04], the PGV constructions, as pointed out in [CDMP05, KM07], do not achieve this level of security.[1]

Our first result divides the 12 secure PGV constructions into two groups $\mathcal{G}_1$ and $\mathcal{G}_2$ of size 6, where within each group the ideal cipher in each construction reduces to the ideal cipher in any other construction (with respect to collision resistance, [everywhere] preimage resistance, and preimage awareness). We sometimes call these the PGV_1-group and the PGV_2-group respectively: these two schemes are representatives of their respective groups. Across different groups, however, and for any of the security games, starting with the ideal cipher we can derive a blockcipher which makes all schemes in one group secure, whereas any scheme in the other group becomes insecure under this blockcipher. This separates the PGV_1-group and the PGV_2-group in terms of *direct* ideal-cipher reducibility. In direct reducibility we use the blockcipher in question without any modifications in another construction. This was one of the reasons to investigate different PGV constructions in the first place. For *free* reductions allowing arbitrary transformations $\mathcal{T}$ of the blockcipher, we show that the PGV constructions can be seen as transformations of each other, and under suitable $\mathcal{T}$ all 12 PGV constructions reduce to each other.

Preneel et al. [PGV94] already discussed equivalence classes from an attack perspective. Our work reaffirms these classes and puts them on a solid theoretical foundation. Dividing the 12 constructions into two groups allows

[1] This, and other points discussed within the body, motivates why we chose the oracle reducibility notion of [BF11] rather than the indifferentiability reducibility notion in [MRH04].

us to say that, within each group, one can use a blockcipher in a construction under the same *qualitative* assumptions on the blockcipher as for schemes; only across the groups this becomes invalid. In other words, the sets (or more formally, distributions) of "good" blockciphers for the groups are not equal, albeit they clearly share the ideal cipher as a common member making both groups simultaneously secure. We note that our results are also *quantitatively* tight in the sense that the blockciphers within a group are proven to be tightly reducible to each other in terms of the number of queries, running times, and success probabilities.

PGV AND DOUBLE-BLOCK-LENGTH HASHING. Double-block-length (DBL) hash or compression functions aim at surpassing the $2^{n/2}$ upper bound for collision resistance of the PGV constructions by using two "PGV-like" constructions in parallel, doubling the output length. There are three major such compression functions, namely, Tandem-DM (TDM, [LM92]), Abreast-DM (ADM, [LM92]), and Hirose's construction (HDM, [Hir06]). Several results underline the optimality of collision-resistance [Hir06, LK11, LSS11] and preimage-resistance bounds [AFK$^+$11] for these functions in the ICM.

Continuing with ideal-cipher reducibility, we establish a connection between the basic PGV constructions and the double-block-length compression functions. Since all the DBL constructions have a "PGV_1-part" (with twice the key size) built in, it follows that any collision for any of the DBL functions immediately yields a collision for PGV_1 built from a blockcipher with $2n$-bit key. In other words, the ideal cipher in the DBL constructions directly reduces to the one in double-key PGV_1. We also prove that there is a free reduction to single-key PGV_1 from this double-key variant, thereby relating DBL functions to PGV_1 for free transformations. It follows, via a free reduction to PGV_1 and a free reduction from PGV_1 to PGV_2, that DBL functions reduce to PGV_2 for free transformations. An analogous result also applies to the everywhere preimage-resistance game, but, somewhat curiously, we show such a result cannot hold for the (standard) preimage-resistance game.

When it comes to free reducibility from PGV to DBL functions, we present irreducibility results for the collision-resistance and [everywhere] preimage-resistance games. We achieve this by making use of an interesting relationship to (lower bounds for) hash combiners [Her05, HKN$^+$05, Pie08]. Namely, if one can turn a collision (or preimage) for, say, PGV_1 into one for a DBL compression function, then we can think of PGV_1, which has n-bit digests, as a sort of robust hash combiner for the DBL function (which has $2n$-bit outputs). However, known lower bounds for hash combiners [Pie08] tell us that such a combiner (with tight bounds and being black box) cannot exist, and this transfers to ideal-cipher reducibility. More in detail, by combining Pietrzak's techniques [Pie08] with a lower bound on generic collision finders by Bellare and Kohno [BK04] on compression functions, we confirm the irreducibility result formally for the simple case of black-box reductions making only a single call to the PGV collision-finder oracle (as also discussed in [Pie08]). We leave the analysis of the full case to the final version. In summary, not only do the DBL functions provide stronger guarantees in terms of quantitative security (as well as efficiency and output length), but they also provably rely on qualitatively weaker assumptions on the blockcipher for the collision-resistance and everywhere preimage-resistance games.

Finally, we demonstrate that for none of the aforementioned DBL constructions the ideal cipher directly reduces to the one in either of the other schemes. That is, starting with the ideal cipher, for each target DBL function we construct a blockcipher which renders it insecure but preserves collision resistance for the other two functions. We are not aware of an analogous result for free reductions, but can exclude transformations which are involutions.

PRACTICAL IMPLICATIONS. Our results show that there is "no clear winner" among the PGV constructions in the sense that one construction always relies on weaker assumptions about the blockcipher than the other ones and should be therefore preferred in practice. This depends on the blockcipher in question. As expressed above, settling this for a specific blockcipher may be tedious, though. Nonetheless, our results do show that DBL constructions are superior in this regard, and that one may switch between PGV constructions of the same group in order to match other practical stipulations.

2 Preliminaries

NOTATION. We write $x \leftarrow y$ for assigning value y to variable x. We write $x \leftarrow\!\!\$\ \mathsf{X}$ for sampling x from (finite) set X uniformly at random. If $\mathcal{A}$ is a probabilistic algorithm we write $y \leftarrow\!\!\$\ \mathcal{A}(x_1, \ldots, x_n)$ for the action of running $\mathcal{A}$ on inputs $x_1, \ldots, x_n$ with coins chosen uniformly at random, and assigning the result to y. We use "|" for string concatenation, denote the bit complement of $x \in \{0,1\}^\star$ by $\overline{x}$. We set $[n] := \{1, \ldots, n\}$. We say $\epsilon(\lambda)$ is negligible if $|\epsilon(\lambda)| \in \lambda^{-\omega(1)}$.

BLOCKCIPHERS. A blockcipher with key length k and block length n is a set of permutations and their inverses on $\{0,1\}^n$ indexed by a key in $\{0,1\}^k$. This set can therefore be thought of as a pair of functions

$$\mathsf{E} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n \quad \text{and} \quad \mathsf{E}^{-1} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n .$$

We denote the set of all such blockciphers by $\mathsf{Block}(k,n)$. A blockcipher is efficient if the above functions can be implemented by an efficient Turing machine.

IDEAL AND IDEALIZED (BLOCK)CIPHERS. An idealized (block)cipher with key length k and block length n is a distribution $\mathcal{E}$ on $\mathsf{Block}(k,n)$. We often consider an $\mathcal{E}$-idealized model of computation where all parties are given oracle access to a blockcipher chosen according to $\mathcal{E}$. *The* ideal-cipher model is the $\mathcal{E}$-idealized model where $\mathcal{E}$ is the uniform distribution on $\mathsf{Block}(k,n)$. We denote the set of all idealized ciphers with key length k and block length n (i.e., the set of all distributions on $\mathsf{Block}(k,n)$) by $\mathsf{Ideal}(k,n)$. Below, when saying that one has oracle access to an idealized cipher $\mathcal{E}$ it is understood that a blockcipher is sampled according to $\mathcal{E}$ and that one gets oracle access to this blockcipher.

COMPRESSION FUNCTIONS. A compression function is a function mapping $\{0,1\}^l$ to $\{0,1\}^m$ where $m < l$. We are primarily interested in compression functions which are built from a blockcipher. In this case we write $\mathsf{F}^{\mathsf{E},\mathsf{E}^{-1}} : \{0,1\}^l \to \{0,1\}^m$. A compression function is often considered in an idealized model where its oracles are sampled according to an idealized cipher $\mathcal{E}$.

2.1 Security notions for compression functions

We now recall a number of fundamental security properties associated with blockcipher-based hashing.

Definition 2.1 (Everywhere preimage and collision resistance [RS04]) *Let $\mathsf{F}^{\mathsf{E},\mathsf{E}^{-1}} : \{0,1\}^l \to \{0,1\}^m$ be a compression function with oracle access to a blockcipher in $\mathsf{Block}(k,n)$. Let $\mathcal{E}$ denote an idealized cipher on $\mathsf{Block}(k,n)$. The preimage- (resp., everywhere preimage-, resp., collision-) resistance advantage of an adversary $\mathcal{A}$ in the $\mathcal{E}$-idealized model against $\mathsf{F}^{\mathsf{E},\mathsf{E}^{-1}}$ are defined by*

$$\mathbf{Adv}^{\mathsf{pre}}_{\mathsf{F},\mathcal{E}}(\mathcal{A}) := \Pr\left[\mathsf{F}^{\mathsf{E},\mathsf{E}^{-1}}(X') = Y \ : \ (\mathsf{E},\mathsf{E}^{-1}) \leftarrow\!\!\$\ \mathcal{E}; X \leftarrow\!\!\$\ \{0,1\}^l; Y \leftarrow \mathsf{F}^{\mathsf{E},\mathsf{E}^{-1}}(X); X' \leftarrow\!\!\$\ \mathcal{A}^{\mathsf{E},\mathsf{E}^{-1}}(Y)\right] ,$$

$$\mathbf{Adv}^{\mathsf{epre}}_{\mathsf{F},\mathcal{E}}(\mathcal{A}) := \Pr\left[\mathsf{F}^{\mathsf{E},\mathsf{E}^{-1}}(X) = Y \ : \ (\mathsf{E},\mathsf{E}^{-1}) \leftarrow\!\!\$\ \mathcal{E}; (Y,\mathrm{st}) \leftarrow\!\!\$\ \mathcal{A}_1; X \leftarrow\!\!\$\ \mathcal{A}_2^{\mathsf{E},\mathsf{E}^{-1}}(\mathrm{st})\right] ,$$

$$\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F},\mathcal{E}}(\mathcal{A}) := \Pr\left[X_0 \neq X_1 \wedge \mathsf{F}^{\mathsf{E},\mathsf{E}^{-1}}(X_0) = \mathsf{F}^{\mathsf{E},\mathsf{E}^{-1}}(X_1) \ : \ (\mathsf{E},\mathsf{E}^{-1}) \leftarrow\!\!\$\ \mathcal{E}; (X_0,X_1) \leftarrow\!\!\$\ \mathcal{A}^{\mathsf{E},\mathsf{E}^{-1}}\right] .$$

For the set S_q of all adversaries which place at most q queries to their E or E^{-1} oracles in total we define

$$\mathbf{Adv}^{\mathsf{pre}}_{\mathsf{F},\mathcal{E}}(q) := \max_{\mathcal{A} \in S_q} \left\{ \mathbf{Adv}^{\mathsf{pre}}_{\mathsf{F},\mathcal{E}}(\mathcal{A}) \right\} ,$$

and similarly for the everywhere preimage-resistance and collision-resistance games. We note that although a compression function cannot be collision resistant nor everywhere preimage resistance with respect to a *fixed* blockcipher, reducibility arguments still apply [Rog06].

Some of our results also hold for "more advanced" properties of hash or compression functions like preimage awareness [DRS09]. (The definition can be found in Appendix A.) If so, we mention this briefly.

2.2 Reducibility

In order to define what it means for an idealized cipher to reduce to another, we begin with a semantics for security games similar to that in [BR06]. We capture the three security properties above by our notion, but can also extend the framework to cover a larger class of security games, such as complex multi-stage games and simulation-based notions. In the simpler case, we will consider a game between a challenger or a game Game and a sequence $\mathcal{A}_1, \mathcal{A}_2, \ldots$ of admissible adversaries (e.g., those which run in polynomial time). When the game terminates by outputting 1, this is deemed a success for the adversary (in that instance of the game). To determine the overall success of the adversaries, we then measure the success probability with respect to threshold t (e.g., 0 for computational games, or $\frac{1}{2}$ for decisional games). We present our formalism in the concrete setting. However, our definitions can be easily extended to the asymptotic setting by letting the game, its parameters, and adversaries to depend on a security parameter.

Definition 2.2 (Secure $\mathcal{E}$-idealized games) *An $\mathcal{E}$-idealized game consists of an oracle Turing machine* Game *(also called the challenger) with access to an idealized cipher $\mathcal{E}$ and n adversary oracles, a threshold $t \in [0,1]$, and a set S of n-tuples of admissible adversaries. The game terminates by outputting a bit. The advantage of adversaries $\mathcal{A}_1, \ldots, \mathcal{A}_n$ against* Game *is defined as*

$$\mathbf{Adv}_{\mathcal{E}}^{\mathsf{Game}}(\mathcal{A}_1, \ldots, \mathcal{A}_n) := \left| \Pr\left[\mathsf{Game}^{\mathsf{E},\mathsf{E}^{-1},\mathcal{A}_1^{\mathsf{E},\mathsf{E}^{-1}},\ldots,\mathcal{A}_n^{\mathsf{E},\mathsf{E}^{-1}}} = 1 \right] - t \right| ,$$

where the probability is taken over the coins of Game*, $\mathcal{A}_1, \ldots, \mathcal{A}_n$, and $(\mathsf{E}, \mathsf{E}^{-1}) \leftarrow\!\!\$\ \mathcal{E}$. For bounds $\epsilon \in [0,1]$ and $T, Q \in \mathbb{N}$ we say* Game *is* (Q, T, ϵ)-secure *if*

$$\forall (\mathcal{A}_1, \ldots, \mathcal{A}_n) \in S : \mathbf{Adv}_{\mathcal{E}}^{\mathsf{Game}}(\mathcal{A}_1, \ldots, \mathcal{A}_n) \leq \epsilon$$

and Game *together with any set of admissible adversaries runs in time at most T and makes at most Q queries to the sample of the idealized cipher, including those of the adversaries.*

For example, the above notion captures everywhere preimage resistance by having $\mathcal{A}_1$ terminate by outputting (Y, st) with no access to the blockcipher, and $\mathcal{A}_2^{\mathsf{E},\mathsf{E}^{-1}}(\mathrm{st})$ return some X; the challenger then outputs 1 if and only if $\mathsf{F}^{\mathsf{E},\mathsf{E}^{-1}}(X) = Y$. Note that in particular, the construction F is usurped, together with the everywhere preimage experiment, in the general notation Game. We also note that with the above syntax we can combine multiple games into one by having a "master" adversary $\mathcal{A}$ first send a label to the challenger deciding which subgame to play and then invoking the corresponding parties and game. Note also that as in [BF11] we assume that an idealized cipher can be given as an entirely ideal object, as a non-ideal object through a full description of an efficient Turing machine given as input to the parties, or a mixture thereof.

IDEAL-CIPHER TRANSFORMATIONS. A transformation of ideal ciphers is a function $\mathcal{T}$ which maps a blockcipher from $\mathsf{Block}(k, n)$ to another blockcipher in $\mathsf{Block}(k', n')$. Typically, we will only be interested in *efficient* transformations i.e., those which can be implemented by efficient oracle Turing machines in the $\mathcal{E}$-idealized model, written $\mathcal{T}^{\mathsf{E}}$. Note that the requirement of $\mathcal{T}$ being a function implies that, algorithmically, the oracle Turing machine is deterministic and stateless. Below we envision the (single) transformation $\mathcal{T}$ to work in different modes $\mathsf{Enc}, \mathsf{Dec}$ to provide the corresponding interfaces for a blockcipher $(\mathsf{E}', \mathsf{E}'^{-1})$. Slightly abusing notation, we simply write $\mathcal{T}$ and $\mathcal{T}^{-1}$ for the corresponding interfaces E' and E'^{-1} (instead of $\mathcal{T}_{\mathsf{Enc}}^{\mathsf{E},\mathsf{E}^{-1}}$ for E' and $\mathcal{T}_{\mathsf{Dec}}^{\mathsf{E},\mathsf{E}^{-1}}$ for E'^{-1}). The transformation is written as

$$\mathsf{E}'(K, M) := \mathcal{T}^{\mathsf{E},\mathsf{E}^{-1}}(K, M) \quad \text{and} \quad \mathsf{E}'^{-1}(K, M) := \mathcal{T}^{-1\,\mathsf{E},\mathsf{E}^{-1}}(K, M) .$$

Any transformation $\mathcal{T}$ also induces a mapping from $\mathsf{Ideal}(k, n)$ to $\mathsf{Ideal}(k', n')$. When E is sampled according to $\mathcal{E}$, then $\mathcal{T}$ induces an idealized cipher $\mathcal{E}' \in \mathsf{Ideal}(k', n')$ which we occasionally denote by $\mathcal{T}^{\mathcal{E}}$.

Definition 2.3 (Ideal-cipher reducibility) *Let* Game_1 *and* Game_2 *be two idealized games relying on blockciphers in* $\mathsf{Block}(k,n)$ *and* $\mathsf{Block}(k',n')$ *respectively. We say* the idealized cipher in Game_2 reduces to the idealized cipher in Game_1*, if for any* $\mathcal{E}_1 \in \mathsf{Ideal}(k,n)$ *there is a deterministic, stateless, and efficient transformation* $\mathcal{T} : \mathsf{Block}(k,n) \to \mathsf{Block}(k',n')$ *such that if*

$$\forall(\mathcal{A}_{1,1},\ldots,\mathcal{A}_{1,n_1}) \in S_1 \;:\; \mathbf{Adv}^{\mathsf{Game}_1}_{\mathcal{E}_1}(\mathcal{A}_{1,1},\ldots,\mathcal{A}_{1,n_1}) \le \epsilon_1\,,$$

whenever Game_1 *runs in time at most* t_1 *and makes at most* Q_1 *queries to the block cipher sampled according to* $\mathcal{E}_1$*, then setting* $\mathcal{E}_2 := \mathcal{T}^{\mathcal{E}_1}$*, we have that*

$$\forall(\mathcal{A}_{2,1},\ldots,\mathcal{A}_{2,n_2}) \in S_2 \;:\; \mathbf{Adv}^{\mathsf{Game}_2}_{\mathcal{E}_2}(\mathcal{A}_{2,1},\ldots,\mathcal{A}_{2,n_2}) \le \epsilon_2\,,$$

where Game *runs in time at most* t_2 *and makes at most* Q_2 *queries to the blockcipher sampled according to* $\mathcal{E}_2$*. In this case we say the reduction is* $(Q_1/Q_2, T, t_1/t_2, \epsilon_1/\epsilon_2)$*-tight, where* T *is an upper bound on the number of queries that* $\mathcal{T}$ *places to its oracle per invocation. When* $k = k'$*,* $n = n'$*, and* $\mathcal{T}$ *is the identity transformation, we say the reduction is* direct*; else it is called* free*.*

DEFINITIONAL CHOICES. In this work, our focus is on reducibility among blockcipher-based hash functions. In this setting, there are often no assumptions beyond the idealized cipher being chosen from a certain distribution. In this case, the strict, strong, and weak reducibility notions as discussed in [BF11] all collapse to the one given above. Of particular interest to us are two types of transformations. First, *free* transformations which can be arbitrary, and second the identity/dummy transformation which does not change the cipher. This latter type of direct reducibility asks if any idealized cipher making one construction secure makes the other secure too. The former type, however, apart from appropriately modifying the syntactical aspects of the blockcipher (such as the key or the block size), asks if the *model* for which one primitive is secure can be reduced to the model for which the other is secure.

RELATIONSHIP WITH INDIFFERENTIABILITY. Ideal-cipher reducibility can be seen in relation with reducibility of systems in the indifferentiability framework [MRH04]. In this framework one says system $\mathcal{U}$ reduces to system $\mathcal{V}$ if there is a deterministic B such that for all cryptosystems $\mathcal{C}$ we have that $\mathcal{C}(B(\mathcal{V}))$ is at least as secure as $\mathcal{C}(\mathcal{U})$. Viewing $\mathcal{C}$ as a security game, indifferentiability reducibility can be seen as oracle reducibility with respect to *all* single-stage games simultaneously. In contrast, we are concerned with a small number of fixed games. In fact this restriction is hard to avoid, as the PGV compression functions themselves do not behave like a random function given access to E *and* E^{-1}; see [CDMP05, KM07]. Also, as demonstrated in [RSS11], the indifferentiability framework does not cover arbitrary multi-stage security games well, whereas we can easily cast them in our framework.

3 Reducibility among the PGV Functions

We start by recalling the blockcipher-based constructions of hash functions by Preneel et al. [PGV94, BRSS10]. The PGV compression functions rely on a blockcipher $\mathsf{E} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, and map $\{0,1\}^{2n}$ to $\{0,1\}^n$:

$$\mathsf{PGV}^{\mathsf{E}}_i : \{0,1\}^{2n} \to \{0,1\}^n \quad \text{for} \quad \mathsf{E} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n\,.$$

There are 64 basic combinations to build such a compression function, of which 12 were first believed [PGV94] (under category "✓" or "FP") and later actually proven to be secure [BRSS10] (under category "group-1"). We denote these secure compression functions by $\mathsf{PGV}_1,\ldots,\mathsf{PGV}_{12}$ and adopt the s-index of [BRSS10] (as defined in Figure 2 there); they are depicted in Figure 1. It is worthwhile mentioning that PGV_1 is known as Matyas–Meyer–Oseas (MMO), PGV_2 as Miyaguchi–Preneel, and PGV_5 as Davies–Meyer (DM). The PGV_1 and PGV_5 functions can be instantiated with a blockcipher whose key length and message length are not equal. The remaining functions, however, do not natively support this feature but they can be generalized such that they do [Sta09].

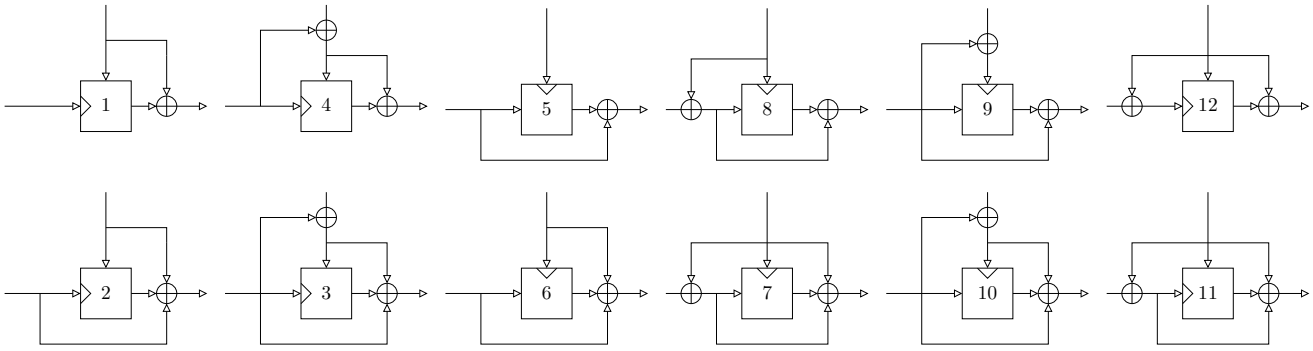


Figure 1: The 12 optimally secure PGV constructions $\mathsf{PGV}_i^{\mathsf{E}}$ for $i \in [12]$. A triangle denotes the location of the key input. When used in an iteration mode, the top input is a message block and the left input is the chaining value. The first (resp. second) row corresponds to the PGV_1-group (resp. PGV_2-group).

For $i \in [12]$ and $q \geq 0$, the security bounds for uniform $\mathcal{E}$ according to [BRS02, Sta09, BRSS10] are

$$\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{PGV}_i,\mathcal{E}}(q) \leq \frac{q^2}{2^n}\,, \qquad \mathbf{Adv}^{\mathsf{pre}}_{\mathsf{PGV}_i,\mathcal{E}}(q) \leq \frac{2q}{2^n}\,, \quad \text{and} \quad \mathbf{Adv}^{\mathsf{epre}}_{\mathsf{PGV}_i,\mathcal{E}}(q) \leq \frac{2q}{2^n}\,.$$

These bounds also hold when the key length and block length are not equal. Furthermore, for uniform $\mathcal{E}$, there exist adversaries $\mathcal{A}$ and $\mathcal{B}$ making q queries to their E and E^{-1} oracles in total such that [BRSS10][2]

$$\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{PGV}_i,\mathcal{E}}(\mathcal{A}) \geq \frac{1}{8e}\frac{q^2+1}{2^n}\,, \qquad \mathbf{Adv}^{\mathsf{pre}}_{\mathsf{PGV}_i,\mathcal{E}}(\mathcal{B}) \geq \frac{q+1}{2^{n+1}}\,, \quad \text{and} \quad \mathbf{Adv}^{\mathsf{epre}}_{\mathsf{PGV}_i,\mathcal{E}}(\mathcal{B}) \geq \frac{q+1}{2^{n+1}}\,.$$

As we will show in the two following theorems, when it comes to ideal-cipher reducibility, the 12 secure PGV constructions can be further partitioned into two subgroups as follows, which we call the PGV_1-group and PGV_2-group, respectively.

$$\mathcal{G}_1 := \{\mathsf{PGV}_1, \mathsf{PGV}_4, \mathsf{PGV}_5, \mathsf{PGV}_8, \mathsf{PGV}_9, \mathsf{PGV}_{12}\} \qquad \mathcal{G}_2 := \{\mathsf{PGV}_2, \mathsf{PGV}_3, \mathsf{PGV}_6, \mathsf{PGV}_7, \mathsf{PGV}_{10}, \mathsf{PGV}_{11}\}$$

The PGV_1 and PGV_2 functions will be representative of their respective groups.

The next proposition shows that, within a group, the compression functions are ideal-cipher reducible to each other in a direct and tight way (i.e., with the identity transformation and preserving the security bounds). It is worth pointing out that Preneel et al. [PGV94] already discussed equivalence classes from an attack perspective. Present work reaffirms these classes and puts them on a solid theoretical foundation. As noted before, we cannot hope that any PGV compression function construction is indifferentiable from random (given access to E and E^{-1}), so we do not cover this property here; we can, however, include the notion of preimage awareness [DRS09] to the games which are preserved.

Proposition 3.1 *Any two PGV constructions in $\mathcal{G}_1$ (resp., in $\mathcal{G}_2$) directly and $(1,1,1,1)$-tightly reduce the idealized cipher to each other for the [everywhere] preimage-resistance, collision-resistance, and preimage-awareness games.*

Proof. This is straightforward for [everywhere] preimage resistance and collision resistance. To see this, observe that there is a syntactical one-to-one correspondence with respect to the inputs within any two functions in each group. Relabeling variables immediately turns any collision (or preimage) for one function into one for the other function. For the sake of concreteness, we consider the collision-resistance ideal-cipher reducibility from $\mathsf{PGV}_5^{\mathcal{E}}$ to $\mathsf{PGV}_1^{\mathcal{E}}$ where for any $(\mathsf{E}, \mathsf{E}^{-1})$ sampled according to $\mathcal{E}$ we have

$$\mathsf{PGV}_1^{\mathsf{E}}(K, M) := \mathsf{E}(K, M) \oplus M \quad \text{and} \quad \mathsf{PGV}_5^{\mathsf{E}}(K, M) := \mathsf{E}(M, K) \oplus K\,.$$

[2]The "plus one" terms are introduced in order to compactly capture the zero-query lower bounds.

Assume towards contradiction that there is an adversary which outputs a $\mathsf{PGV}_5^{\mathsf{E}}$ collision $(X, Y) \neq (X', Y')$ for this E. Turn this collision into $(Y, X) \neq (Y', X')$, and output it as a $\mathsf{PGV}_1^{\mathsf{E}}$ collision. It is clear that

$$\mathsf{PGV}_1^{\mathsf{E}}(Y, X) = \mathsf{E}(Y, X) \oplus X = \mathsf{E}(Y', X') \oplus X' = \mathsf{PGV}_1^{\mathsf{E}}(Y', X')\,,$$

where the inner equality holds whenever the alleged $\mathsf{PGV}_5^{\mathsf{E}}$ adversary succeeds. Since this holds for *any* E the claim also follows for any distribution $\mathcal{E}$ on such blockciphers.

For preimage resistance of the same compression functions, the reduction would again simply turn a preimage (X, Y) into (Y, X).

As for preimage awareness, if an adversary $\mathcal{A}_5$ against $\mathsf{PGV}_5^{\mathsf{E}}$ is able to break preimage awareness by outputting (X, Y), we could easily turn this into an adversary $\mathcal{A}_1$ against $\mathsf{PGV}_1^{\mathsf{E}}$ by returning (Y, X). Any extractor $\mathcal{X}_1$ refuting a successful attack of $\mathcal{A}_1$ could be, vice versa, turned into an extractor $\mathcal{X}_5$ against $\mathcal{A}_5$ by swapping the components of $\mathcal{X}_1$'s outputs. □

Note that since we can combine the individual games into one, we can conclude that any blockcipher making a scheme from one group secure for all games simultaneously, would also make any other scheme in the group simultaneously secure. Also, the above equivalence still holds for PGV_1 and PGV_5 in case they work with a blockcipher with different key and message length.

The next theorem separates the two groups with respect to the collision-resistance and [everywhere] preimage-resistance games.

Theorem 3.2 *No PGV construction in $\mathcal{G}_1$ (resp., in $\mathcal{G}_2$) directly reduces to any PGV construction in $\mathcal{G}_2$ (resp., in $\mathcal{G}_1$) for any of the collision-resistance and [everywhere] preimage-resistance games.*

For collision resistance and preimage resistance we assume the ideal cipher, whereas for everywhere preimage resistance we only need the minimal property that there exists *some* blockcipher making the schemes in one group secure, in order to achieve the separation. Due to space constraints we present the proof in Appendix B.

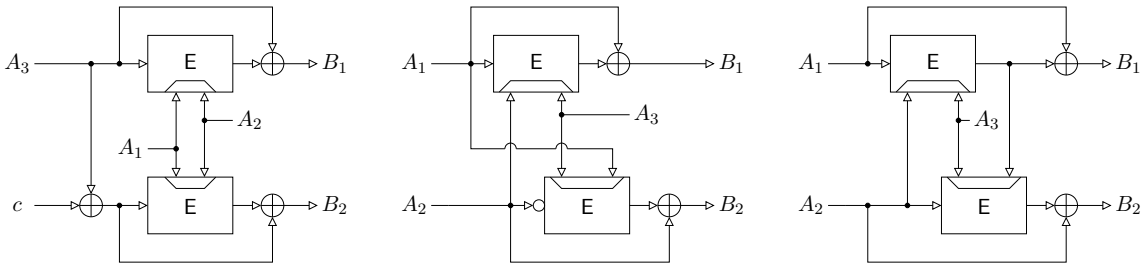
Proposition 3.3 *Any two PGV constructions PGV_i and PGV_j for $i, j \in [12]$ $(1, 1, 1, 1)$-tightly reduce the idealized cipher to each other for the [everywhere] preimage-resistance and collision-resistance games (under free transformations).*

To prove this, we first show that there is a transformation such that there is an inter-group reduction, i.e., $\mathsf{PGV}_2 \in \mathcal{G}_2$ reduces to $\mathsf{PGV}_1 \in \mathcal{G}_1$ and vice versa—indeed we will use the same transformation for either direction. By transitivity we then obtain a reduction for any two constructions through Proposition 3.1, where we may view the identity transformation as a special case of an arbitrary one.

Proof. Consider PGV_1 and PGV_2. We claim that for the transformation defined through

$$\mathcal{T}^{\mathsf{E}}(K, M) := \mathsf{E}(K, M) \oplus K \quad \text{and} \quad {\mathcal{T}^{-1}}^{\mathsf{E}^{-1}}(K, C) := \mathsf{E}^{-1}(K, C \oplus K)\,,$$

the security of $\mathsf{PGV}_2^{\mathcal{T}^{\mathsf{E}}}$ reduces to $\mathsf{PGV}_1^{\mathsf{E}}$. This is because both compression functions are identical for any E, implying that the idealized cipher $\mathcal{T}^{\mathcal{E}}$ reduces to the idealized cipher $\mathcal{E}$. This can be easily done vice versa, too, for the same transformation, noting that applying $\mathcal{T}$ twice is the identity transformation. Observe that $\mathcal{T}^{\mathsf{E}}$ is indeed a permutation for any fixed key K; the statement now trivially follows. □



(2.a) Hirose-DM (2.b) Abreast-DM (2.c) Tandem-DM

Figure 2: The three double-block-length compression functions. The hollow circle in Abreast-DM denotes bitwise complement.

4 Double-Block-Length Hashing and PGV

4.1 Reducibility from DBL to PGV

In this section we study the relation between three prominent double-block-length hash function constructions in the literature, namely, Hirose-DM [Hir04, Hir06], Abreast-DM [LM92, LK11], and Tandem-DM [LM92, LSS11, FGL09a], and the PGV constructions. All the DBL compression functions under consideration here map $3n$-bit inputs to $2n$-bit outputs, and rely on a blockcipher with $2n$-bit keys and n-bit block. More precisely, these constructions are of the form

$$\mathsf{F}^{\mathsf{E}} : \{0,1\}^{3n} \to \{0,1\}^{2n} \quad \text{where} \quad \mathsf{E} : \{0,1\}^{2n} \times \{0,1\}^{n} \to \{0,1\}^{n}\,.$$

We denote the Hirose-DM for a constant $c \in \{0,1\}^n \setminus \{0^n\}$, the Abreast-DM, and the Tandem-DM compression functions by HDM_c, ADM, and TDM, respectively. These functions are defined as follows (see Figure 2 for pictorial representations).

$$\begin{aligned}
\mathsf{HDM}_c^{\mathsf{E}}(A_1, A_2, A_3) &:= (\mathsf{E}(A_1|A_2, A_3) \oplus A_3, \mathsf{E}(A_1|A_2, A_3 \oplus c) \oplus A_3 \oplus c)\\
\mathsf{ADM}^{\mathsf{E}}(A_1, A_2, A_3) &:= \big(\mathsf{E}(A_2|A_3, A_1) \oplus A_1, \mathsf{E}(A_3|A_1, \overline{A_2}) \oplus A_2\big)\\
\mathsf{TDM}^{\mathsf{E}}(A_1, A_2, A_3) &:= (\mathsf{E}(A_2|A_3, A_1) \oplus A_1, \mathsf{E}(A_3|\mathsf{E}(A_2|A_3, A_1), A_2) \oplus A_2)
\end{aligned}$$

The next proposition shows that collisions (resp., somewhere preimages) in HDM_c directly lead to collisions (resp., somewhere preimages) for the double-key versions of PGV_1 and PGV_5 functions.

Proposition 4.1 *The idealized ciphers in* HDM_c*, for any* $c \in \{0,1\}^n \setminus \{0^n\}$*,* ADM*, and* TDM *compression functions directly and* $(1,1,1,1)$*-tightly reduce to those in the (double-key versions of the)* PGV_1 *and* PGV_5 *functions for the everywhere preimage-resistance and collision-resistance games.*

Proof. We only treat the case of PGV_1 as reducibility to PGV_5 is proved similarly. Note that the first component of any of the DBL constructions is a PGV_1 value (up to relabeling of the variables). This means that any adversary breaking the collision resistance of, say, HDM_c can be used to break the collision resistance of PGV_1. A similar argument applies to the everywhere preimage-resistance game. We take the output of a first-stage adversary which returns an image value for HDM_c and pass its first component out as the candidate image point for PGV_1. When the second stage of the adversary outputs a preimage, we also use it as our own guess. □

Note that despite the tightness of the reduction, a blockcipher that makes the schemes PGV_1 and PGV_5 ideally secure is not guaranteed to make the double-block-length compression functions secure beyond the implied single-length security bound.

Curiously, the above argument fails for the preimage-resistance game as we cannot extend a challenge value for PGV_1 to a full challenge value for a DBL construction. The proof of the following proposition appears in Appendix C.

Proposition 4.2 *The idealized cipher in none of the DBL constructions directly reduces to the idealized cipher in* PGV_1 *(and hence neither to the one in* PGV_5*) for the (standard) preimage-resistance game.*

Direct ideal-cipher reducibility to the other PGV constructions is not syntactically possible as only the PGV_1 and PGV_5 constructions can be natively instantiated with a double-block-length blockcipher.[3] Note that the above proposition leaves open the (im)possibility of free reductions from DBL to PGV, which we leave to future work.

We next show that under *free* transformations a double-block-length instantiation of PGV_1 reduces to a single-block-length instantiation of PGV_1. By the transitivity of reductions we obtain reducibility of the idealized cipher in the DBL constructions to that in any of the PGV constructions.

Proposition 4.3 *The idealized cipher in* PGV_1 *instantiated with an idealized cipher in* $\mathsf{Ideal}(2n, n)$ $(2, 2, 1, 1)$*-tightly reduces to the one in* PGV_1 *when instantiated with an idealized cipher in* $\mathsf{Ideal}(n, n)$ *for the everywhere preimage-resistance and collision-resistance games.*

Proof. We define the required transformation as follows.

$$\mathcal{T}^{\mathsf{E},\mathsf{E}^{-1}}(K_1|K_2, M) := \mathsf{E}(\mathsf{E}(K_1, K_2) \oplus K_2, M) \qquad \mathcal{T}^{-1\,\mathsf{E},\mathsf{E}^{-1}}(K_1|K_2, C) := \mathsf{E}^{-1}(\mathsf{E}(K_1, K_2) \oplus K_2, C)$$

Note that the above transformed blockcipher, when used in PGV_1 with twice the key length, yields a fixed-length Merkle–Damgård (MD) iteration using a random initialization vector of PGV_1 for cipher E (with single key length):

$$\mathsf{PGV}_1^{\mathcal{T}^{\mathsf{E}}}(K_1|K_2, M) = \mathsf{PGV}_1^{\mathsf{E}}(\mathsf{PGV}_1^{\mathsf{E}}(K_1, K_2), M)\,.$$

As shown in, say [ANPS07], this MD chaining preserves both collision resistance and everywhere preimage resistance of $\mathsf{PGV}_1^{\mathsf{E}}$ (but requires two blockcipher calls per evaluation). This proves the proposition. □

REMARK. Although Merkle–Damgård chaining does *not* in general preserve the preimage resistance of the underlying compression function, there exist more sophisticated chaining rules, such as ROX [ANPS07], which do so. If such chaining rules are used to compress the keys in the proposition above, we also obtain reducibility for the preimage-resistance game.

4.2 Separations among the DBL compression functions

We now investigate direct reducibility among the DBL compression functions, as well as PGV_1 and DBL functions. We focus on collision resistance, but similar techniques (for separations) may be applicable to the other security games. For this game, there are twelve relations to be considered, three of which have already been settled by Proposition 4.1. We study the remaining relations by providing separations among all the possible pairs. In doing so, we give blockciphers E such that one of the DBL constructions (and hence by Proposition 4.1 the PGV_1 function, too) admits a trivial collision, whereas the other two constructions are *simultaneously* secure.

We start with the HDM_c compression function where $c \neq 0^n$. Let E be a blockcipher. Define a modified blockcipher $\tilde{\mathsf{E}}$ as follows.

$$M_c := \mathsf{E}^{-1}(0^n|0^n, \mathsf{E}(0^n|0^n, 0^n) \oplus c)\,, \quad C_0 := \mathsf{E}(0^n|0^n, 0^n)\,, \quad C_c := \mathsf{E}(0^n|0^n, c)\,.$$

[3] There exist modifications of the PGV constructions which can be instantiated with DBL blockciphers [Sta09]. We leave their treatment to future work.

$$\tilde{\mathsf{E}}(K_1|K_2,M) := \begin{cases} C_0 \oplus c & \text{if } (K_1|K_2,M) = (0^n|0^n,c)\,; \\ C_c & \text{if } (K_1|K_2,M) = (0^n|0^n,M_c)\,; \\ \mathsf{E}(K_1|K_2,M) & \text{otherwise.} \end{cases}$$

$$\tilde{\mathsf{E}}^{-1}(K_1|K_2,C) := \begin{cases} c & \text{if } (K_1|K_2,C) = (0^n|0^n,C_0 \oplus c)\,; \\ M_c & \text{if } (K_1|K_2,C) = (0^n|0^n,C_c)\,; \\ \mathsf{E}^{-1}(K_1|K_2,C) & \text{otherwise.} \end{cases}$$

Note that $\tilde{\mathsf{E}}$ and $\tilde{\mathsf{E}}^{-1}$ above define a blockcipher and we have $c \neq 0^n$. Hence,

$$\mathsf{HDM}_c^{\tilde{\mathsf{E}}}(0^n,0^n,0^n) = (\tilde{\mathsf{E}}(0^n|0^n,0^n) \oplus 0^n, \tilde{\mathsf{E}}(0^n|0^n,c) \oplus c) = (C_0, C_0 \oplus c \oplus c) = (C_0,C_0)\,,$$
$$\mathsf{HDM}_c^{\tilde{\mathsf{E}}}(0^n,0^n,c) = (\tilde{\mathsf{E}}(0^n|0^n,c) \oplus c, \tilde{\mathsf{E}}(0^n|0^n,0^n) \oplus 0^n) = (C_0 \oplus c \oplus c, C_0) = (C_0,C_0)\,.$$

and the pair $((0^n,0^n,0^n),(0^n,0^n,c))$ thus constitutes a non-trivial collision for $\mathsf{HDM}_c^{\tilde{\mathsf{E}}}$. However, the next lemma shows that ADM and TDM remain collision resistant for this cipher. The proof appears in Appendix D.

Lemma 4.4 *Let $\tilde{\mathsf{E}}$ be a blockcipher as above with a distribution according to $(\mathsf{E},\mathsf{E}^{-1}) \leftarrow\!\!\$\ \mathsf{Block}(2n,n)$. Then $\mathsf{ADM}^{\tilde{\mathsf{E}}}$ and $\mathsf{TDM}^{\tilde{\mathsf{E}}}$ are both collision resistant.*

Due to space constraints we provide the remaining separating examples in Appendix D.

Theorem 4.5 *Let $c \in \{0,1\}^n \setminus \{0^n\}$. Then among the compression functions HDM_c, ADM, and TDM neither one directly reduces the idealized cipher in either one of the other two functions for the collision-resistance game.*

As a corollary of the above results we get that there is no direct reduction from PGV to any of the DBL compression functions: otherwise we also obtain direct reducibility to any other DBL compression function via Theorem 4.1, which we have shown to be impossible in the above theorem. In the next section we will extend this irreducibility result to free reductions.

4.3 Irreducibility of PGV to DBL

We now turn our attention to the converse of Propositions 4.1 and 4.3: can one convert any idealized cipher which makes a DBL construction secure to one which makes a PGV construction secure? We show strong evidence towards the impossibility of such a reduction. To this end, we restrict the class of reductions under the construction to *black-box* ones [RTV04]. Such a reduction is a pair of oracle Turing machines $(\mathcal{T},\mathcal{R})$. Both machines have access to a blockcipher, $\mathcal{T}$ is a transformation which implements an idealized cipher, and $\mathcal{R}$ is a reduction which given oracle access to an algorithm $\mathcal{B}$ breaking the security of a PGV construction when instantiated with $\mathcal{T}^{\mathsf{E}}$, breaks the security of a DBL construction with respect to E (for random E). As it will become apparent from the proof of the theorem, the type of reductions that we actually rule out allow both the transformation and the reduction to depend on the blockcipher and hence, in the terminology of [RTV04], the class of reductions that we rule out lies somewhere in between fully black-box and $\forall\exists$semi-black-box reductions. More concisely, this class is captured as an NBN reduction in the CAP taxonomy of [BBF13], meaning that the *C*onstruction may make non-black-box use of primitive, and that the reduction makes black-box use of the *A*dversary resp. non-black-box use of the *P*rimitive.

We make two further simplifications on the structure of the reduction. First we assume that $\mathcal{R}$ queries its break oracle $\mathcal{B}$ once. We call this a single-query reduction. Second, we require the reduction to succeed with a constant probability whenever $\mathcal{B}$ is successful. Now, the intuition behind the impossibility of the existence of such a reduction follows that for lower bounds on the output size of hash combiners [Pie08]. The underlying idea is that the collision-resistance security of any of the DBL constructions is *beyond* that of the PGV constructions. More precisely, around $\Theta(2^n)$ queries are needed to break the collision resistance of any of the DBL constructions with

	$\mathcal{G}_1$	$\mathcal{G}_2$	TDM	HDM_c	ADM
$\mathcal{G}_1$	Y 3.1	N 3.2	Y 4.1	Y 4.1	Y 4.1
$\mathcal{G}_2$	N 3.2	Y 3.1	–	–	–
TDM	N 4.5	–	Y	N 4.5	N 4.5
HDM_c	N 4.5	–	N 4.5	Y	N 4.5
ADM	N 4.5	–	N 4.5	N 4.5	Y

(3.a) Results for the identity transformation.

	$\mathcal{G}_1$	$\mathcal{G}_2$	TDM	HDM_c	ADM
$\mathcal{G}_1$	Y $\rightarrow$	Y 3.3	Y $\rightarrow$	Y $\rightarrow$	Y $\rightarrow$
$\mathcal{G}_2$	Y 3.3	Y $\rightarrow$	Y $\star$	Y $\star$	Y $\star$
TDM	N 4.6	N 4.6	Y	n 4.5	n 4.5
HDM_c	N 4.6	N 4.6	n 4.5	Y	n 4.5
ADM	N 4.6	N 4.6	n 4.5	n 4.5	Y

(3.b) Results for arbitrary transformations.

Figure 3: Summary of our reducibility results for collision resistance. A "Y" or "N" in a cell means that any cipher which makes the compression function corresponding to the row collision resistant also makes the compression function corresponding to the column collision resistant. A "–" in direct reductions indicates a syntax mismatch. The number below an entry indicates the theorem/proposition supporting the claim. An arrow "$\rightarrow$" means that the result is implied by the left table. Reductions on the diagonal of TDM, HDM_c, and ADM trivially follow by self-reductions. Note that for arbitrary transformations each cell might be using different transformations. The star symbol "$\star$" denotes reducibility by transitivity. An "n" is a separation for a restricted class of transformations; see Section 5.

noticeable probability, whereas this bound is only $\Theta(2^{n/2})$ for the PGV constructions. To derive a contradiction, we may simulate the break algorithm $\mathcal{B}$ for the reduction with only $\Theta(2^{n/2})$ queries, and the reduction will translate this collision efficiently to a DBL construction collision, which contradicts the $\Theta(2^n)$ collision-resistance bound.

We are now ready to state our irreducibility theorem. Since we are dealing with an impossibility result, for the sake of clarity of the presentation we present the theorem in asymptotic language. The proof appears in Appendix E.

Theorem 4.6 *There is no single-query fully black-box ideal-cipher reduction from any of the PGV constructions to any of the DBL constructions for the collision-resistance and [everywhere] preimage-resistance games as long as the reduction is tight: when the number of queries, run times, and success probabilities are parameterized by a security parameter, the reduction is* $(\mathcal{O}(1), \mathcal{O}(1), \mathcal{O}(1), \mathcal{O}(1))$*-tight.*

It is conceivable that the techniques of [Pie08] can be leveraged to derive a more general theorem which rules out reductions that call the break oracle multiple times. Furthermore, one might also be able to extended the result to arbitrary games for two given constructions, as long as a lower bound on the success probability of an attack on the security of the first construction is noticeably higher than an upper bound on the security of the second.

5 Summary and Future Work

We summarize our reducibility results in Figure 3 and refer to the caption for details. One important observation from these results is that we do not have one single "Y" column, i.e., a compression function which reduces to all of the other ones—or, equivalently, a compression function which is secure if any of the others is secure. This would be a clear winner in the sense that it is the safest choice for practice.

For the "n" entries of Table 3.b we can show that there is a separation for a large class of potential transformation functions. More specifically, we show that there is no surjective transformation $\mathcal{T}$ to reduce, say, ADM to HDM_{1^n}, as long as the transformation also preserves HDM-security "backwards." Here, surjectivity means that $\mathcal{T}^{\mathsf{E}}$ varies over all possible blockciphers if E runs through all blockciphers, and backward security preservation means that $\mathcal{E}$ is secure for HDM if $\mathcal{T}^{\mathcal{E}}$ is. Transformations which are covered by this include, for example, those of the form $\mathcal{T}^{\mathsf{E}}_{\pi_1,\pi_2}(K_1|K_2, M) = \pi_2(\mathsf{E}(K_1|K_2, \pi_1(M)))$ for fixed involutions π_1, π_2 over $\{0,1\}^n$, or more generally, any

transformation which is an involution (over $\mathsf{Block}(2n, n)$).[4] The argument is as follows. Assume that there exists such a $\mathcal{T}$. Then for any blockcipher E which makes HDM secure, the blockcipher $\mathcal{T}^{\mathsf{E}}$ makes ADM secure. However, we also know that there is a blockcipher $\mathsf{E}^\star$ such that $\mathsf{E}^\star$ gives rise to a collision-resistant $\mathsf{HDM}_{1^n}^{\mathsf{E}^\star}$ but renders $\mathsf{ADM}^{\mathsf{E}^\star}$ collision tractable (see Appendix D). Now define E to be any blockcipher in the preimage of $\mathsf{E}^\star$ under $\mathcal{T}$ (such an E exists as $\mathcal{T}$ is surjective). The transformation now maps E to $\mathsf{E}^\star$, which means that it fails to provide security for ADM. Furthermore, E makes $\mathsf{HDM}_{1^n}^{\mathsf{E}}$ collision resistant by assumption about backward security. This, however, contradicts the requirement of reducibility from ADM to HDM, because E makes HDM secure but $\mathcal{T}^{\mathsf{E}}$ is insecure for ADM.

OPEN PROBLEMS. Recall that we showed that one can transform a good blockcipher E (or rather distribution $\mathcal{E}$) for the PGV_1-group into a good one $\mathcal{T}^{\mathsf{E}}$ for the PGV_2-group. We also presented a transformation in the opposite direction. Ideally, though, one would be interested in a *single* transformation $\mathcal{T}$ which, given $\mathcal{E}$ making a PGV construction secure, turns it into $\mathcal{T}^{\mathcal{E}}$ which *simultaneously* makes both the PGV_1-group and the PGV_2-group secure. Such a transformation would be of interest because incorporating it into the compression function would result in a construction that relies on a weaker assumption than either just PGV_1 or PGV_2. Consequently, it would provide a handle to *strengthen* existing schemes (in a provable way). Note that such a result would not contradict the separation of direct reducibility between the PGV_1-group and the PGV_2-group, because simultaneous security looks for a (transformed) cipher in the intersection of good (distributions over) blockciphers for both groups. This intersection is clearly non-empty because it contains the ideal cipher; the question to address here is how hard it is to hit a distribution when starting with the minimal security assumption that (a potentially non-ideal) $\mathcal{E}$ is good for at least one PGV construction. We remark our technique of separating the DBL constructions from PGV_1 does not seem to apply here, as the simultaneous security bound for PGV_1 and PGV_2 is $\Theta(q^2/2^n)$. However, surjective, backward-secure transformations are still ruled out according to the same argument as in the HDM vs. ADM case.

Another direction of research left open here is the existence of reductions among two compression functions for *different* games. For example, one might ask whether the collision resistance of one construction for a blockcipher gives preimage resistance in another (or perhaps the same) construction with the same cipher. In particular, using Simon's result [Sim98] one might be able to demonstrate the impossibility of reducing collision resistance to preimage resistance for any of the PGV constructions.

Finally, let us emphasize that all results in this work apply directly to compression functions. Needless to say, in practice compression functions are iterated in order to hash arbitrary lengths of data. This could extend the set of $\mathcal{E}$ that provide security, potentially changing the scope for transformations between constructions. We leave the question of the existence of reductions among iterated hash functions as an interesting open problem.

Acknowledgments

The work described in this paper has been supported in part by the European Commission through the ICT programme under contract ICT-2007-216676 ECRYPT II. Paul Baecher and Pooya Farshim are supported by grant Fi 940/4-1 of the German Research Foundation (DFG). Marc Fischlin is supported by grant Fi 940/3-1 of the German Research Foundation (DFG).

References

[AFK+11] Frederik Armknecht, Ewan Fleischmann, Matthias Krause, Jooyoung Lee, Martijn Stam, and John P. Steinberger. The preimage security of double-block-length compression functions. In Dong Hoon

[4] An example of a surjective transformation which is not backward secure for PGV_1 is $\mathcal{T}^{\mathsf{E}}(K, M) = \mathsf{E}(K, M) \oplus K$, because it maps PGV_1 for $\mathcal{T}^{\mathsf{E}}$ to PGV_2 for E, and we know that there are idealized ciphers making PGV_2 secure but PGV_1 insecure.

Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 233–251. Springer, December 2011. (Cited on pages 3 and 25.)

[ANPS07] Elena Andreeva, Gregory Neven, Bart Preneel, and Thomas Shrimpton. Seven-property-preserving iterated hashing: ROX. In Kaoru Kurosawa, editor, *ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 130–146. Springer, December 2007. (Cited on page 10.)

[BBF13] Paul Baecher, Christina Brzuska, and Marc Fischlin. Notions of black-box reductions, revisited. Cryptology ePrint Archive, Report 2013/101, 2013. `http://eprint.iacr.org/`. (Cited on page 11.)

[BF11] Paul Baecher and Marc Fischlin. Random oracle reducibility. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 21–38. Springer, August 2011. (Cited on pages 2, 5, and 6.)

[BK04] Mihir Bellare and Tadayoshi Kohno. Hash function balance and its impact on birthday attacks. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 401–418. Springer, May 2004. (Cited on pages 3, 26, and 27.)

[BK09] Alex Biryukov and Dmitry Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 1–18. Springer, December 2009. (Cited on page 2.)

[BKN09] Alex Biryukov, Dmitry Khovratovich, and Ivica Nikolic. Distinguisher and related-key attack on the full AES-256. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 231–249. Springer, August 2009. (Cited on page 2.)

[BR06] Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 409–426. Springer, May / June 2006. (Cited on page 5.)

[BRS02] John Black, Phillip Rogaway, and Thomas Shrimpton. Black-box analysis of the block-cipher-based hash-function constructions from PGV. In Moti Yung, editor, *CRYPTO 2002*, volume 2442 of *LNCS*, pages 320–335. Springer, August 2002. (Cited on pages 1 and 7.)

[BRSS10] John Black, Phillip Rogaway, Thomas Shrimpton, and Martijn Stam. An analysis of the blockcipher-based hash functions from PGV. *Journal of Cryptology*, 23(4):519–545, October 2010. (Cited on pages 1, 2, 6, 7, 17, and 20.)

[CDMP05] Jean-Sébastien Coron, Yevgeniy Dodis, Cécile Malinaud, and Prashant Puniya. Merkle-Damgård revisited: How to construct a hash function. In Victor Shoup, editor, *CRYPTO 2005*, volume 3621 of *LNCS*, pages 430–448. Springer, August 2005. (Cited on pages 2 and 6.)

[DRS09] Yevgeniy Dodis, Thomas Ristenpart, and Thomas Shrimpton. Salvaging Merkle-Damgård for practical applications. In Antoine Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 371–388. Springer, April 2009. (Cited on pages 2, 4, 7, and 16.)

[FGL09a] Ewan Fleischmann, Michael Gorski, and Stefan Lucks. On the security of tandem-DM. In Orr Dunkelman, editor, *FSE 2009*, volume 5665 of *LNCS*, pages 84–103. Springer, February 2009. (Cited on page 9.)

[FGL09b] Ewan Fleischmann, Michael Gorski, and Stefan Lucks. Security of cyclic double block length hash functions. In Matthew G. Parker, editor, *12th IMA International Conference on Cryptography and Coding*, volume 5921 of *LNCS*, pages 153–175. Springer, December 2009. (Cited on page 25.)

[FLS+08] Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The skein hash function family, 2008. (Cited on page 1.)

[GKM+11] Praveen Gauravaram, Lars R. Knudsen, Krystian Matusiewicz, Florian Mendel, Christian Rechberger, Martin Schläfffer, and Soren S. Thomsen. Grøstl — a SHA-3 candidate, 2011. (Cited on page 1.)

[Her05] Amir Herzberg. On tolerant cryptographic constructions. In Alfred Menezes, editor, *CT-RSA 2005*, volume 3376 of *LNCS*, pages 172–190. Springer, February 2005. (Cited on page 3.)

[Hir04] Shoichi Hirose. Provably secure double-block-length hash functions in a black-box model. In Choonsik Park and Seongtaek Chee, editors, *ICISC 04*, volume 3506 of *LNCS*, pages 330–342. Springer, December 2004. (Cited on page 9.)

[Hir06] Shoichi Hirose. Some plausible constructions of double-block-length hash functions. In Matthew J. B. Robshaw, editor, *FSE 2006*, volume 4047 of *LNCS*, pages 210–225. Springer, March 2006. (Cited on pages 3 and 9.)

[HKN+05] Danny Harnik, Joe Kilian, Moni Naor, Omer Reingold, and Alon Rosen. On robust combiners for oblivious transfer and other primitives. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 96–113. Springer, May 2005. (Cited on page 3.)

[Kho10] Dmitry Khovratovich. *New Approaches to the Cryptanalysis of Symmetric Primitives*. PhD thesis, University of Luxembourg, 2010. (Cited on page 2.)

[KM07] Hidenori Kuwakado and Masakatu Morii. Indifferentiability of single-block-length and rate-1 compression functions. *IEICE Transactions*, 90-A(10):2301–2308, 2007. (Cited on pages 2 and 6.)

[LK11] Jooyoung Lee and Daesung Kwon. The security of abreast-dm in the ideal cipher model. *IEICE Transactions*, 94-A(1):104–109, 2011. (Cited on pages 3, 9, 22, and 25.)

[LM92] Xuejia Lai and James L. Massey. Hash function based on block ciphers. In Rainer A. Rueppel, editor, *EUROCRYPT'92*, volume 658 of *LNCS*, pages 55–70. Springer, May 1992. (Cited on pages 3 and 9.)

[LSS11] Jooyoung Lee, Martijn Stam, and John P. Steinberger. The collision security of tandem-DM in the ideal cipher model. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 561–577. Springer, August 2011. (Cited on pages 3, 9, 23, and 25.)

[MRH04] Ueli M. Maurer, Renato Renner, and Clemens Holenstein. Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In Moni Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 21–39. Springer, February 2004. (Cited on pages 2 and 6.)

[PGV94] Bart Preneel, René Govaerts, and Joos Vandewalle. Hash functions based on block ciphers: A synthetic approach. In Douglas R. Stinson, editor, *CRYPTO'93*, volume 773 of *LNCS*, pages 368–378. Springer, August 1994. (Cited on pages 1, 2, 6, and 7.)

[Pie08] Krzysztof Pietrzak. Compression from collisions, or why CRHF combiners have a long output. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 413–432. Springer, August 2008. (Cited on pages 3, 11, and 12.)

[Rog06] Phillip Rogaway. Formalizing human ignorance. In Phong Q. Nguyen, editor, *Progress in Cryptology - VIETCRYPT 06*, volume 4341 of *LNCS*, pages 211–228. Springer, September 2006. (Cited on page 4.)

[RS04] Phillip Rogaway and Thomas Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In Bimal K. Roy and Willi Meier, editors, *FSE 2004*, volume 3017 of *LNCS*, pages 371–388. Springer, February 2004. (Cited on pages 2 and 4.)

[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, May 2011. (Cited on page 6.)

[RTV04] Omer Reingold, Luca Trevisan, and Salil P. Vadhan. Notions of reducibility between cryptographic primitives. In Moni Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 1–20. Springer, February 2004. (Cited on page 11.)

[Sim98] Daniel R. Simon. Finding collisions on a one-way street: Can secure hash functions be based on general assumptions? In Kaisa Nyberg, editor, *EUROCRYPT'98*, volume 1403 of *LNCS*, pages 334–345. Springer, May / June 1998. (Cited on page 13.)

[Sta08] Martijn Stam. Beyond uniformity: Better security/efficiency tradeoffs for compression functions. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 397–412. Springer, August 2008. (Cited on page 20.)

[Sta09] Martijn Stam. Blockcipher-based hashing revisited. In Orr Dunkelman, editor, *FSE 2009*, volume 5665 of *LNCS*, pages 67–83. Springer, February 2009. (Cited on pages 6, 7, 10, 20, and 21.)

[WPS+12] Lei Wei, Thomas Peyrin, Przemyslaw Sokolowski, San Ling, Josef Pieprzyk, and Huaxiong Wang. On the (in)security of IDEA in various hashing modes. In Anne Canteaut, editor, *FSE 2012*, volume 7549 of *LNCS*, pages 163–179. Springer, March 2012. (Cited on page 2.)

A Preimage Awareness

Roughly speaking, preimage awareness [DRS09] states that any adversary which comes up with an image Z for a compression function, already knows a preimage X for it. This is formalized though the existence of an extractor algorithm $\mathcal{X}$ which can recover the value X from Z and the list α of previous queries to E and E^{-1}.

Definition A.1 (Preimage awareness [DRS09]) *Let* $\mathsf{F}^{\mathsf{E},\mathsf{E}^{-1}} : \{0,1\}^l \to \{0,1\}^m$ *be a compression function with oracle access to a blockcipher in* $\mathsf{Block}(k,n)$*. Let* $\mathcal{E}$ *denote an idealized cipher on* $\mathsf{Block}(k,n)$*. The preimage awareness advantage of an adversary* $\mathcal{A}$ *with respect to the deterministic extractor* $\mathcal{X}$ *in the* $\mathcal{E}$*-idealized model against* $\mathsf{F}^{\mathsf{E},\mathsf{E}^{-1}}$ *is defined by*

$$\mathbf{Adv}^{\mathsf{pra}}_{\mathsf{F},\mathcal{E},\mathcal{X}}(\mathcal{A}) := \Pr\left[\mathbf{Exp}^{\mathsf{pra}}_{\mathsf{F},\mathcal{E},\mathcal{X}}(\mathcal{A}) = 1\right] ,$$

where $\mathbf{Exp}^{\mathsf{pra}}_{\mathsf{F},\mathcal{E},\mathcal{X}}(\mathcal{A})$ *is shown in Figure 4.*

In [DRS09] it has been shown that the 12 optimally secure PGV constructions are preimage aware in the ideal-cipher model. Vice versa, preimage awareness (for compressing functions) has been shown to imply collision resistance, and help in proving indifferentiability from a random oracle in certain construction [DRS09].

B Proof of Theorem 3.2: $\mathcal{G}_1$/$\mathcal{G}_2$ Separations

Theorem B.1 (Theorem 3.2, restated) *No PGV construction in* $\mathcal{G}_1$ *(resp., in* $\mathcal{G}_2$*) directly reduces to any PGV construction in* $\mathcal{G}_2$ *(resp., in* $\mathcal{G}_1$*) for any of the collision-resistance and [everywhere] preimage-resistance games.*

$\underline{\mathbf{Exp}^{\mathsf{pra}}_{\mathsf{F},\mathcal{E},\mathcal{X}}(\mathcal{A})}$:
$(\mathsf{E},\mathsf{E}^{-1}) \leftarrow_{\$} \mathcal{E}$
$X \leftarrow_{\$} \mathcal{A}^{\mathbf{E},\mathbf{E^{-1}},\mathbf{Ex}}$
$Z \leftarrow \mathsf{F}^{\mathsf{E},\mathsf{E}^{-1}}(X)$
Return $(X \neq \mathsf{V}[Z]$
$\wedge\ \mathsf{Q}[Z] = 1)$

$\underline{\textbf{oracle } \mathbf{E}(K,X)}$:
$Y \leftarrow \mathsf{E}(K,X)$
$\alpha \leftarrow \alpha||(K,X,Y)$
Return Y

$\underline{\textbf{oracle } \mathbf{E^{-1}}(K,Y)}$:
$X \leftarrow \mathsf{E}^{-1}(K,Y)$
$\alpha \leftarrow \alpha||(K,X,Y)$
Return X

$\underline{\textbf{oracle } \mathbf{Ex}(Z)}$:
$\mathsf{Q}[Z] \leftarrow 1$
$\mathsf{V}[Z] \leftarrow \mathcal{X}(Z,\alpha)$
Return $\mathsf{V}[Z]$

Figure 4: Experiment defining preimage awareness.

Proof. Take PGV_1 and PGV_2 as the representatives of their respective groups. Since all the constructions directly reduce to each other within their group, it suffices to separate these two constructions; by transitivity a reduction between any other combination would otherwise contradict the fact that PGV_1 and PGV_2 have been separated. Recall that

$$\mathsf{PGV}_1^{\mathsf{E}}(K,M) := \mathsf{E}(K,M) \oplus M \quad \text{and} \quad \mathsf{PGV}_2^{\mathsf{E}}(K,M) := \mathsf{E}(K,M) \oplus M \oplus K\,.$$

Collision resistance. We first show that the compression functions PGV_1 and PGV_2 do not reduce to each other with respect to collision resistance. In order to prove this, take the ideal cipher $\mathcal{E}$ (with the uniform distribution), which is known to make PGV_2 secure for collision resistance, and let (K_0,M_0) and (K_1,M_1) be from $\{0,1\}^{2n}$ with $K_0 \neq K_1$. We show how to transform any blockcipher E in $\mathsf{Block}(n,n)$ (the support of $\mathcal{E}$) into a new cipher $\tilde{\mathsf{E}}$ such that the induced distribution $\tilde{\mathcal{E}}$ on such blockciphers still makes PGV_2 secure, but for which (K_0,M_0) and (K_1,M_1) form a trivial collision under PGV_1 for any $\tilde{\mathsf{E}}$ sampled from $\tilde{\mathcal{E}}$.

Now for a given blockcipher E and points (K_0,M_0) and (K_1,M_1), define

$$C_1' := \mathsf{E}(K_0,M_0) \oplus M_0 \oplus M_1\,, \quad M_1' := \mathsf{E}^{-1}(K_1,C_1')\,, \quad C_1 := \mathsf{E}(K_1,M_1)\,,$$

and let $\tilde{\mathsf{E}}$ be the blockcipher identical to E, apart from a reprogramming to change the function value for M_1 under key K_1 to C_1', and redirecting the former's preimage M_1' under key K_1 to C_1:

$$\tilde{\mathsf{E}}(K,M) := \begin{cases} C_1' & \text{if } (K,M) = (K_1,M_1)\,; \\ C_1 & \text{if } (K,M) = (K_1,M_1')\,; \\ \mathsf{E}(K,M) & \text{otherwise.} \end{cases} \qquad \tilde{\mathsf{E}}^{-1}(K,C) := \begin{cases} M_1 & \text{if } (K,C) = (K_1,C_1')\,; \\ M_1' & \text{if } (K,C) = (K_1,C_1)\,; \\ \mathsf{E}^{-1}(K,C) & \text{otherwise.} \end{cases}$$

By inspection, $\tilde{\mathsf{E}}$ is again a blockcipher with inverse $\tilde{\mathsf{E}}^{-1}$. Finding a collision for PGV_1 with respect to any $\tilde{\mathsf{E}}$ chosen from a tweaked distribution as above is easy since

$$\mathsf{PGV}_1^{\tilde{\mathsf{E}}}(K_0,M_0) = \tilde{\mathsf{E}}(K_0,M_0) \oplus M_0 = \mathsf{E}(K_0,M_0) \oplus M_0 = C_1' \oplus M_1 = \tilde{\mathsf{E}}(K_1,M_1) \oplus M_1 = \mathsf{PGV}_1^{\tilde{\mathsf{E}}}(K_1,M_1)\,.$$

For the analysis of the collision resistance of $\mathsf{PGV}_2^{\tilde{\mathsf{E}}}$ where $\mathcal{E}$ is ideal, we recall the prototype PGV proof from [BRSS10]. This proof concentrates on the probability that an adversary creates its first collision on the ith query and subsequently uses a union bound to combine these stepwise probabilities. For this proof all that is needed (to bound the probability of a success at step i) is (a) that the ith query corresponds to a single compression function evaluation that (over the randomness of the query's answer) is uniformly distributed over a set of size at least $2^n - i$, and (b) that the adversary only knows at most i compression function evaluations prior to making query i. When using $\tilde{\mathsf{E}}$ instead of a sample E from the ideal cipher, we need to take into account that we have introduced a dependency among the points (K_0,M_0), (K_1,M_1), and (K_1,M_1'). We do this by giving these three queries *for free* to the adversary at the beginning of the collision-finding game. If these three points do not cause a collision among themselves, the original proof goes through as from that moment onwards, (a) $\tilde{\mathsf{E}}$ is identically distributed to the ideal cipher E and (b) the free queries just resulted in three extra compression function evaluations.

For the tweaked points, we look at the $\binom{3}{2} = 3$ possible colliding pairs. Let $C_0 := \mathsf{E}(K_0,M_0)$.

1. The first case is:

$$\mathsf{PGV}_2^{\tilde{\mathsf{E}}}(K_0, M_0) = \mathsf{PGV}_2^{\tilde{\mathsf{E}}}(K_1, M_1) \iff C_0 \oplus M_0 \oplus K_0 = C_1' \oplus M_1 \oplus K_1 \iff K_0 = K_1\,,$$

   which happens with probability 0 since $K_0 \neq K_1$.

2. The second case is:

$$\mathsf{PGV}_2^{\tilde{\mathsf{E}}}(K_0, M_0) = \mathsf{PGV}_2^{\tilde{\mathsf{E}}}(K_1, M_1') \iff C_0 \oplus M_0 \oplus K_0 = C_1 \oplus M_1' \oplus K_1\,.$$

   Adding $C_1 \oplus K_1$ to both sides and enciphering with E under K_1 we get that the equation is equivalent to

$$\mathsf{E}(K_1, C_0 \oplus K_0 \oplus C_1 \oplus K_1 \oplus M_0) = \mathsf{E}(K_0, M_0) \oplus M_0 \oplus M_1\,.$$

   Since $K_0 \neq K_1$ it is clear that the probability of equality is $1/2^n$ as the values of the E on the two sides of the equation are independently and uniformly distributed.

3. The third case is:

$$\mathsf{PGV}_2^{\tilde{\mathsf{E}}}(K_1, M_1) = \mathsf{PGV}_2^{\tilde{\mathsf{E}}}(K_1, M_1') \iff C_1' \oplus M_1 \oplus K_1 = C_1 \oplus M_1' \oplus K_1\,,$$

   which after rearranging as in the previous case becomes equivalent to

$$\mathsf{E}(K_1, C_0 \oplus C_1 \oplus M_0) = \mathsf{E}(K_0, M_0) \oplus M_0 \oplus M_1\,.$$

   Once again, since $K_0 \neq K_1$, we have that the probability of a collision is $1/2^n$.

This proves that the idealized cipher $\tilde{\mathcal{E}}$ makes PGV_2 collision resistant.

For the converse separation, start with the ideal blockcipher $\mathcal{E}'$, which makes PGV_1 secure. For any E' in the support of $\mathcal{E}'$ consider the blockcipher E with $\mathsf{E}(K, M) = \mathsf{E}'(K, M) \oplus K$ and $\mathsf{E}^{-1}(K, C) = \mathsf{E}'^{-1}(K, C \oplus K)$. Since

$$\mathsf{PGV}_2^{\mathsf{E}}(K, M) = \mathsf{E}(K, M) \oplus K \oplus M = \mathsf{E}'(K, M) \oplus M = \mathsf{PGV}_1^{\mathsf{E}'}(K, M)$$

this distribution $\mathcal{E}$ on blockciphers E now makes PGV_2 secure. Furthermore, $\mathcal{E}$ itself is again the uniform distribution on all blockciphers. Run the same transformation from E to $\tilde{\mathsf{E}}$ as above, such that $\mathsf{PGV}_2^{\tilde{\mathsf{E}}}$ remains secure, whereas $\mathsf{PGV}_1^{\tilde{\mathsf{E}}}$ is easy to break. Apply now once more the idea of adding the key to the cipher's output and define $\tilde{\mathsf{E}}'$ through

$$\tilde{\mathsf{E}}'(K, M) = \tilde{\mathsf{E}}(K, M) \oplus K\,, \quad \text{and} \quad \tilde{\mathsf{E}}'^{-1}(K, C) = \tilde{\mathsf{E}}^{-1}(K, C \oplus K)\,,$$

such that again

$$\mathsf{PGV}_2^{\tilde{\mathsf{E}}'}(K, M) = \mathsf{PGV}_1^{\tilde{\mathsf{E}}}(K, M)\,, \quad \text{and} \quad \mathsf{PGV}_2^{\tilde{\mathsf{E}}}(K, M) = \mathsf{PGV}_1^{\tilde{\mathsf{E}}'}(K, M)\,.$$

We conclude that the distribution on blockciphers $\tilde{\mathsf{E}}'$ now makes PGV_1 collision resistant, but any blockcipher allows to find collisions for PGV_2 easily. This proves the separation in the other direction.

Everywhere preimage resistance. For everywhere preimage resistance it is convenient to start with an arbitrary (not necessarily ideal) distribution on blockciphers E which makes PGV_1 secure. We tweak every such E to $\tilde{\mathsf{E}}$ by setting

$$\tilde{\mathsf{E}}(K, M) := \begin{cases} M \oplus K & \text{if } K = \mathsf{E}(0^n, 0^n)\,; \\ \mathsf{E}(K, M) & \text{otherwise.} \end{cases} \qquad \tilde{\mathsf{E}}^{-1}(K, C) := \begin{cases} C \oplus K & \text{if } K = \mathsf{E}(0^n, 0^n)\,; \\ \mathsf{E}^{-1}(K, C) & \text{otherwise.} \end{cases}$$

Obviously $\tilde{\mathsf{E}}$ together with $\tilde{\mathsf{E}}^{-1}$ constitute a blockcipher.

First observe that we can assume $\mathsf{E}(0^n, 0^n) \neq 0^n$, or else any adversary pair outputting 0^n in the first stage and $(0^n, 0^n)$ in the second stage would refute everywhere preimage resistance for $\mathsf{PGV}_1^{\mathsf{E}}$. Hence, the probability that $\mathsf{E}(0^n, 0^n) = 0^n$ must be negligible, and from now on we condition on this event not happening. We can now show that $\mathsf{PGV}_2^{\tilde{\mathsf{E}}}$ is not secure. For this, let $\mathcal{A}_1(1^n)$ output 0^n, and let $\mathcal{A}_2^{\tilde{\mathsf{E}},\tilde{\mathsf{E}}^{-1}}(0^n)$ return $(K, M) := (\tilde{\mathsf{E}}(0^n, 0^n), 0^n)$. Then, since $\tilde{\mathsf{E}}(0^n, 0^n) = \mathsf{E}(0^n, 0^n)$ by assumption about $\mathsf{E}(0^n, 0^n) \neq 0^n$, we conclude that

$$\mathsf{PGV}_2^{\tilde{\mathsf{E}}}(K, M) = \tilde{\mathsf{E}}(K, M) \oplus K \oplus M = \tilde{\mathsf{E}}(\tilde{\mathsf{E}}(0^n, 0^n), 0^n) \oplus \tilde{\mathsf{E}}(0^n, 0^n) = \tilde{\mathsf{E}}(0^n, 0^n) \oplus \tilde{\mathsf{E}}(0^n, 0^n) = 0^n\,.$$

Hence, the adversary pair always finds an image/preimage pair with a single query to $\tilde{\mathsf{E}}$.

Next we show that any pair $(\mathcal{A}_1, \mathcal{A}_2)$ against PGV_1 for $\tilde{\mathsf{E}}$ can be immediately turned into a pair against PGV_1 for E. Assume that $\mathcal{A}_1(1^n)$ returns some (Y, st), and that $\mathcal{A}_2^{\tilde{\mathsf{E}},\tilde{\mathsf{E}}^{-1}}(Y, \mathrm{st})$ finds (K, M) such that $\mathsf{PGV}_1^{\tilde{\mathsf{E}}}(K, M) = Y$. There are two cases: If $K = \mathsf{E}(0^n, 0^n)$, then letting the second adversary $\mathcal{A}_2^{\mathsf{E},\mathsf{E}^{-1}}$ (now against E) return $(0^n, 0^n)$ would yield a preimage of Y under $\mathsf{PGV}_1^{\mathsf{E}}$, because then

$$Y = \mathsf{PGV}_1^{\tilde{\mathsf{E}}}(K, M) = M \oplus \mathsf{E}(0^n, 0^n) \oplus M = \mathsf{E}(0^n, 0^n) = \mathsf{PGV}_1^{\mathsf{E}}(0^n, 0^n)\,.$$

In the other case, i.e., when $K \neq \mathsf{E}(0^n, 0^n)$, it is clear that (K, M) is also a preimage under $\mathsf{PGV}_1^{\mathsf{E}}$. Hence, either case must be negligible, and $\mathsf{PGV}_1^{\tilde{\mathsf{E}}}$ must be secure.

For the converse separation, as in the case of collision resistance, we apply the technique of adding the key once to the innermost blockcipher, and another time to the outer blockcipher. This leads to a separating example for PGV_2 from PGV_1 for the everywhere preimage-resistance game.

Preimage resistance. Finally we treat the case of preimage resistance. Given a blockcipher E sampled from the uniform distribution, we let $M_{K,0} := \mathsf{E}^{-1}(K, 0^n)$, $C_{K,0} := \mathsf{E}(K, 0^n)$ for each key K, and define a tweaked blockcipher $\tilde{\mathsf{E}}$ as follows.

$$\tilde{\mathsf{E}}(K, M) := \begin{cases} 0^n & \text{if } M = 0^n\,; \\ C_{K,0} & \text{if } M = M_{K,0}\,; \\ \mathsf{E}(K, M) & \text{otherwise.} \end{cases} \qquad \tilde{\mathsf{E}}^{-1}(K, C) := \begin{cases} 0^n & \text{if } C = 0^n\,; \\ M_{K,0} & \text{if } C = C_{K,0}\,; \\ \mathsf{E}^{-1}(K, C) & \text{otherwise.} \end{cases}$$

Note that $\mathsf{PGV}_2^{\tilde{\mathsf{E}}}(K, 0^n) = 0^n \oplus 0^n \oplus K = K$. Hence, any adversary which on input Y outputs $(Y, 0^n)$ succeeds with probability 1 in the preimage-resistance game for $\mathsf{PGV}_2^{\tilde{\mathsf{E}}}$. It remains to show that $\mathsf{PGV}_1^{\tilde{\mathsf{E}}}$ is preimage resistant. An adversary cannot succeed by outputting a pair $(K, 0^n)$ since $\mathsf{PGV}_1^{\tilde{\mathsf{E}}}(K, 0^n) = 0^n$, which would arise as a challenge value with only a negligible probability. Similarly, the challenge digest will originate from $(K, M_{K,0})$ for some K with probability 2^{-n} only. Hence any preimage-resistance adversary must either attack PGV_1 with respect to the original cipher E (which we know to be secure) or recover a preimage using the second branch of $\tilde{\mathsf{E}}$, i.e., output a preimage $(K, M_{K,0})$ for

$$\mathsf{PGV}_1^{\tilde{\mathsf{E}}}(K, M_{K,0}) = C_{K,0} \oplus M_{K,0} = \mathsf{E}(K, 0^n) \oplus \mathsf{E}^{-1}(K, 0^n)$$

for some K. Since E is sampled from the ideal cipher, the two summands are uniformly and independently distributed for each K (unless K is queried). Thus, for a given target digest, any attacker will only have a negligible success probability to recover a preimage of this form.

Applying the transformation which reduces $\mathcal{G}_1$ to $\mathcal{G}_2$ to the cipher $\tilde{\mathsf{E}}$ we obtain an idealized cipher under which PGV_1 is not preimage resistant but PGV_1 is. □

C Proof of Proposition 4.2: DBL/PGV Preimage-Resistance Separations

Proposition C.1 (Proposition 4.2, restated) *The idealized cipher in none of the DBL constructions directly reduces to the idealized cipher in* PGV_1 *(and hence neither to the one in* PGV_5*) for the (standard) preimage-resistance game.*

Proof. Let us start with separating HDM_{1^n} (we briefly discuss how to extend the separation to HDM_c for other nonzero values of c at the end). Recall that there is a natural embedding of $\{0,1\}^{n-1}$ in $\mathrm{GF}(2^{n-1})$ where field addition corresponds to computing exclusive-or, and field multiplication is performed modulo a fixed irreducible polynomial. For an $\alpha \in \mathrm{GF}(2^{n-1})\backslash\{0,1\}$, we define a distribution on $\mathsf{Block}(2n,n)$ by picking a cipher $\mathsf{E} \leftarrow\!\!\$\ \mathsf{Block}(n/2-1, n/2-1)$, ignoring the key, and essentially enciphering either the left or the right half of the input block, depending on the most significant bit of the input. That is, we parse the input M as $m_1|M_1|m_2|M_2$, where m_i are bits and M_i are of length $n/2-1$, and set

$$\tilde{\mathsf{E}}(K, m_1|M_1|m_2|M_2) := \begin{cases} 0|\mathsf{E}(0^{n/2-1}, M_1)|m_2|(\alpha M_2) & \text{if } m_1 = 0\,; \\ 1|\mathsf{E}(0^{n/2-1}, M_2)|m_2|(\alpha M_1) & \text{otherwise.} \end{cases}$$

$$\tilde{\mathsf{E}}^{-1}(K, c_1|C_1|c_2|C_2) := \begin{cases} 0|\mathsf{E}^{-1}(0^{n/2-1}, C_1)|c_2|(\alpha^{-1} C_2) & \text{if } c_1 = 0\,; \\ 1|(\alpha^{-1} C_2)|c_2|\mathsf{E}^{-1}(0^{n/2-1}, C_1) & \text{otherwise.} \end{cases}$$

It is not too difficult to check that $\tilde{\mathsf{E}}$ and $\tilde{\mathsf{E}}^{-1}$ as above define a blockcipher. To see that HDM_{1^n} is not preimage resistant with respect to the distribution on such $\tilde{\mathsf{E}}$, note that with probability $1/4$ in the preimage-resistance game we have that $m_1 = m_2 = 0$, in which case

$$\begin{aligned} &\mathsf{HDM}^{\tilde{\mathsf{E}}}_{1^n}(A_1, A_2, 0|M_1|0|M_2) = \\ &\quad = \Big(0|(\mathsf{E}(0^{n/2-1}, M_1) \oplus M_1)|0|(\alpha M_2 \oplus M_2), 1|(\mathsf{E}(0^{n/2-1}, \overline{M_2}) \oplus \overline{M_1})|1|(\alpha \overline{M_1} \oplus \overline{M_2})\Big)\ . \end{aligned}$$

Now given a preimage-resistance challenge value as shown above, we can recover M_2 from the second part of the first component, $(\alpha+1)M_2$. Note that here we use that $\alpha \neq 1$ and thus $\alpha + 1 \neq 0$ over the field of characteristic 2. Then using M_2 and the second part of the second component we can also recover M_1. The tuple $(0^n, 0^n, 0|M_1|0|M_2)$ is a valid preimage (note that A_1 and A_2 do not affect the value of the compression function).

It remains to show that $\mathsf{PGV}_1^{\tilde{\mathsf{E}}}$ for such distributed blockciphers $\tilde{\mathsf{E}}$ is preimage resistant. Note that

$$\mathsf{PGV}_1^{\tilde{\mathsf{E}}}(K, m_1|M_1|m_2|M_2) := \begin{cases} 0|(\mathsf{E}(0^{n/2-1}, M_1) \oplus M_1)|0|(\alpha M_2 \oplus M_2) & \text{if } m_1 = 0\,; \\ 0|(\mathsf{E}(0^{n/2-1}, M_2) \oplus M_1)|0|(\alpha M_1 \oplus M_2) & \text{otherwise.} \end{cases}$$

For preimage resistance, observe that the K and m_2 inputs and the 0s in the output can be discarded (cf. [Sta08, Lemma 3]), so for the preimage resistance of $\mathsf{PGV}_1^{\tilde{\mathsf{E}}}$ we can instead regard the two functions

$$\begin{aligned} \mathsf{F}_0^{\mathsf{E}}(M_1|M_2) &:= (\mathsf{E}(0^{n/2-1}, M_1) \oplus M_1)|(\alpha M_2 \oplus M_2)\ , \\ \mathsf{F}_1^{\mathsf{E}}(M_1|M_2) &:= (\mathsf{E}(0^{n/2-1}, M_2) \oplus M_1)|(\alpha M_1 \oplus M_2)\ . \end{aligned}$$

Using techniques similar to those from [BRSS10, Section 10], one can prove that for either function the uniform distribution for $(M_1|M_2)$ together with the uniform distribution $\mathcal{E}$ for E, induce a close to uniform distribution over the possible challenge digests. Consequently, if both $\mathsf{F}_0^{\mathsf{E}}$ and $\mathsf{F}_1^{\mathsf{E}}$ are everywhere preimage resistant, then $\mathsf{PGV}_1^{\mathsf{E}}$ is preimage resistant (as the adversary against $\mathsf{PGV}_1^{\mathsf{E}}$ needs to find a preimage of a randomly selected digest under either $\mathsf{F}_0^{\mathsf{E}}$ or $\mathsf{F}_1^{\mathsf{E}}$). For the preimage resistance of $\mathsf{F}_0^{\mathsf{E}}$ it suffices to observe that $M_1 \mapsto \mathsf{E}(0^{n/2-1}, M_1) \oplus M_1$ is well known to be everywhere preimage resistant (e.g., [Sta09, Theorem 6]) as appending $(\alpha M_2 \oplus M_2)$ does not affect the

security (it is independent of M_1). To prove that $\mathsf{F}_1^{\mathsf{E}}$ is also preimage resistant, we start by considering the auxiliary compression function

$$\mathsf{F}^{\mathsf{E}}(M) := \mathsf{E}(0^k, M) \oplus (\alpha^{-1} \cdot M) \quad \text{for} \quad \alpha \neq 0\,.$$

This function is preimage resistant for an ideally distributed E (which follows from [Sta09, Theorem 6]). We now show that any preimage-resistance adversary $\mathcal{A}$ against $\mathsf{F}_1^{\mathsf{E}}$ can be used to break the preimage resistance of F^{E}. Given a challenge value Z for F^{E}, choose $Y_2 \leftarrow\!\!\$\ \{0,1\}^{n/2-1}$, set $Y_1 := Z \oplus Y_2$, and run $\mathcal{A}(0|Y_1, 0|\alpha Y_2)$. By a simple code expansion, the challenge value $(Y_1, \alpha Y_2)$ can be seen as being generated by choosing a random (K, M_2) and computing $(\mathsf{E}(0^k, M_2) \oplus M_1, \alpha M_1 \oplus M_2)$ where $M_1 := \alpha^{-1} M_2 \oplus Y_2$. Note that M_1 is uniformly distributed and is independent of (K, M_2). Hence when $\mathcal{A}$ returns a successful preimage (M_1, M_2), the second component, M_2, would be a valid preimage for Z.

We briefly discuss how to extend the above argument to HDM_c for other nonzero values of c. To this end, we need to ensure that adding c in the second component has the same effect of flipping the first bit of the input as above. We do this by first noting the position, i_c, of the most significant nonzero bit of c. Instead of differentiating the two branches of the cipher based on m_1 we do this by inspecting m_{i_c} and leak this bit accordingly. The remaining bits are then used to form what was M_1 and M_2 before.

We now give an idealized cipher separating the preimage resistance of ADM from that of PGV_1. For any blockcipher in $\mathsf{Block}(n/2, n/2)$, define the function $f^{\mathsf{E}}(X) := \mathsf{E}(0^{n/2}, X) \oplus X$. It is straightforward to show that this function is one way in the presence of E and E^{-1} oracles sampled uniformly from $\mathsf{Block}(n/2, n/2)$. With notation as in the previous example, and denoting the most significant bit of K by $\mathrm{msb}(K)$, based on f^{E} we define the following blockcipher.

$$\tilde{\mathsf{E}}(K_{11}|K_{12}|K_{21}|K_{22}, M_1|M_2) := \begin{cases} (f^{\mathsf{E}}(K_{12}) \oplus M_1)|\alpha M_2 & \text{if } \mathrm{msb}(K_{11}) = 0\,; \\ (f^{\mathsf{E}}(K_{22}) \oplus M_1)|\alpha M_2 & \text{if } \mathrm{msb}(K_{11}) = 1\,. \end{cases}$$

$$\tilde{\mathsf{E}}^{-1}(K_{11}|K_{12}|K_{21}|K_{22}, C_1|C_2) := \begin{cases} (f^{\mathsf{E}}(K_{12}) \oplus C_1)|\alpha^{-1} C_2 & \text{if } \mathrm{msb}(K_{11}) = 0\,; \\ (f^{\mathsf{E}}(K_{22}) \oplus C_1)|\alpha^{-1} C_2 & \text{if } \mathrm{msb}(K_{11}) = 1\,. \end{cases}$$

Observe that $\tilde{\mathsf{E}}$ and $\tilde{\mathsf{E}}^{-1}$ as above define a permutation for each key and hence constitute a blockcipher. Let us now look at $\mathsf{ADM}^{\tilde{\mathsf{E}}}$ values conditioned on the event that $\mathrm{msb}(A_{21}) = 0 \wedge \mathrm{msb}(A_{31}) = 1$ which occurs with probability $1/4$ for randomly chosen A_2 and A_3:

$$\mathsf{ADM}^{\tilde{\mathsf{E}}}(A_{11}|A_{12}, A_{21}|A_{22}, A_{31}|A_{32}) = \left(f^{\mathsf{E}}(A_{22})|(\alpha A_{12} \oplus A_{12}), f^{\mathsf{E}}(A_{12}) \oplus 1^{n/2}|(\alpha \overline{A_{22}} \oplus A_{22})\right)\,.$$

Clearly $\mathsf{ADM}^{\tilde{\mathsf{E}}}$ is not preimage resistant in this case as all the values on which the compression depends can be read off from the digest value. More specifically, given such a value in the preimage-resistance game, the point $(0^{n/2}|A_{12}, 0^{n/2}|A_{22}, 0^n)$ is a valid preimage. To see that $\mathsf{PGV}_1^{\tilde{\mathsf{E}}}$ is preimage resistant for such blockciphers (over the choice of E) observe that any successful preimage-resistance adversary can be immediately used to invert f^{E}, which we have discussed is one way in the ideal-cipher model.

Finally, it turns out that the above blockcipher also separates the preimage resistance of TDM from that of PGV_1: whenever $\mathrm{msb}(A_{21}) = 0$ and $\mathrm{msb}(A_{31}) = 1$ (which happens, again, with probability $1/4$ in the preimage game) we have that

$$\mathsf{TDM}^{\tilde{\mathsf{E}}}(A_{11}|A_{12}, A_{21}|A_{22}, A_{31}|A_{32}) = \left(f^{\mathsf{E}}(A_{22})|(\alpha A_{12} \oplus A_{12}), f^{\mathsf{E}}(\alpha A_{12})|(\alpha \overline{A_{22}} \oplus A_{22})\right)\,,$$

from which a preimage value can be readily computed since α is public. For the sake of concreteness, a preimage is given by $(0^{n/2}|A_{12}, 0^{n/2}|A_{22}, 0^n)$. The fact that the distribution of blockciphers $\tilde{\mathsf{E}}$ preserves preimage resistance for PGV_1 has been shown before, concluding the proof. $\square$

D Proofs of Lemma 4.4 and Theorem 4.5: DBL Separations

Lemma D.1 (Lemma 4.4, restated) *Let* $\tilde{\mathsf{E}}$ *be a blockcipher as defined in Section 4.2 with a distribution according to* $(\mathsf{E}, \mathsf{E}^{-1}) \leftarrow\!\!\$\ \mathsf{Block}(2n, n)$. *Then* $\mathsf{ADM}^{\tilde{\mathsf{E}}}$ *and* $\mathsf{TDM}^{\tilde{\mathsf{E}}}$ *are both collision resistant.*

Proof. We consider ADM where we first recall the existing proof of collision resistance in the ideal-cipher model by Lee and Kwon [LK11]. We will argue that with only minor modifications, their proof goes through also for the almost ideal cipher $\tilde{\mathsf{E}}$. The original proof relies on the observation that queries to the blockcipher can be grouped into cycles by taking into account how they can be used to evaluate the ADM compression function. Suppose an adversary wants to evaluate $\mathsf{ADM}^{\mathsf{E}}(A_1, A_2, A_3)$. This requires the queries $\mathsf{E}(A_2|A_3, A_1)$ and $\mathsf{E}(A_3|A_1, \overline{A_2})$ to be made. Here the second query is intended for the evaluation of the lower half of Fig. (2.b), but it could also be used in the upper half, as part of the evaluation of $\mathsf{ADM}^{\mathsf{E}}(\overline{A_2}, A_3, A_1)$. In that case, the lower-half query would be $\mathsf{E}(A_1|\overline{A_2}, \overline{A_3})$. Now this query could also be used in the upper half, leading to lower-half query $\mathsf{E}(\overline{A_2}|\overline{A_3}, \overline{A_1})$. It might seem that this could go on for a while, but after $\mathsf{E}(\overline{A_3}|\overline{A_1}, A_2)$ and $\mathsf{E}(\overline{A_1}|A_2, A_3)$, the next query in this sequence is $\mathsf{E}(A_2|A_3, A_1)$ which we already saw at the very beginning. Thus after at most six steps the cycle is complete; moreover, when distinct, the six blockcipher queries within a cycle uniquely determine six ADM compression function evaluation and they are not used for any other ADM evaluations. This observation is used in the proof by limiting a collision-finding adversary to querying full cycles only: whenever he makes a query, he will get the remaining queries in the cycle for free. For this modified adversary, Lee and Kwon subsequently bound both the probability of finding a collision within a single cycle and the probability of finding a collision between cycles.

For the analysis of the collision resistance of $\mathsf{ADM}^{\tilde{\mathsf{E}}}$ (where E is ideal) we need to take into account possible interdependencies among $(0^n|0^n, 0^n)$, $(0^n|0^n, c)$, or $(0^n|0^n, M_c)$. As in our modified PGV proof, we will give these three queries for free to the adversary, but in line with the Lee–Kwon proof, we will then have to give *the full cycles* of these points for free as well. For concreteness, these cycles are of the form

$$\{(0^n|0^n, x), (0^n|x, 1^n), (x|1^n, 1^n), (1^n|1^n, \overline{x}), (1^n|\overline{x}, 0^n), (\overline{x}|0^n, 0^n)\}$$

where $x \in \{0^n, c, M_c\}$. It is not always the case that the three choices for x lead to distinct cycles, but this is not an issue. Once we have established that these initial free queries do not cause a collision, the Lee–Kwon proof kicks in (where the free cycles only affect the number of queries made so far).

To ease bounding the probability of a collision due to the free cycles, we will give the corresponding queries for free in a particular order, starting with $\tilde{\mathsf{E}}(0^n|0^n, 0^n)$ and $\tilde{\mathsf{E}}(0^n|0^n, 1^n)$. Potentially both these points are affected by our tweaking (if $1^n \in \{c, M_c\}$), but these two queries only lead to a single compression function evaluation, which is insufficient to find a collision. For the remaining four queries in this cycle it is easy to check that the key will be distinct from $0^n|0^n$, so the outcomes will be as for the ideal cipher. When made in order, the third query leads to one additional compression function evaluation; the probability (over the randomness of the answer of the third query) that this is the same as the already known $\mathsf{ADM}(0^n, 0^n, 0^n)$ is 2^{-n}. The probability the fourth query leads to a success is at most $\frac{2}{2^n}$ (as there are now two targets to aim for and the key is fresh), the fifth query at most $\frac{3}{2^n-1}$ (as the key has been used once before) and the sixth query at most $\frac{2\cdot 4}{2^n}$ (as it adds two compression function evaluations). For the second cycle, first give query $\tilde{\mathsf{E}}(0^n|0^n, c)$ for free (if $c = 1^n$, move straight to the next cycle). This query on its own cannot add a compression function evaluation, thus it cannot lead to a collision. The remaining queries in the cycle all use non-$(0^n|0^n)$ keys so with similar arguments as for the first cycle, the probability of creating a collision is bounded by $\frac{6}{2^n}$, $\frac{7}{2^n}$, $\frac{8}{2^n-2}$, $\frac{9}{2^n}$, and $\frac{20}{2^n}$ respectively. For the third cycle, start with $\tilde{\mathsf{E}}(0^n|0^n, M_c)$ (if $M_c \in \{1^n, c\}$ this query has already been made at a point where it could not have caused a collision and we are already done). Again, as single query in a cycle it cannot lead to a collision; and all the remaining queries in the cycles each have probability at most $\frac{32}{2^n}$ of creating a collision. Taking a union bound leads to a probability of at most $\frac{150}{2^n-2}$ of the free cycles leading to a collision in $\mathsf{ADM}^{\tilde{\mathsf{E}}}$, which is negligible (for increasing n). This concludes the proof that $\mathsf{ADM}^{\tilde{\mathsf{E}}}$ is collision resistant.

For the analysis of $\mathsf{TDM}^{\tilde{\mathsf{E}}}$ we recall the proof by Lee et al. [LSS11]. In fact, they give two proofs: a short, elegant, and tight one and a second, more tedious and less tight one (in the full version only). As we are not interested in tightness at this point, we will use the second proof as our starting point, as it is easier to adapt for our purposes (in particular, it does not modify the adversary). The proof introduces various auxiliary events that bound the number of certain "bad" configurations, and proceeds by showing that (a) the probability of a collision being found when these auxiliary events do not occur is small,[5] and (b) the probability of these auxiliary events occurring is small.

When we move from the ideal cipher to $\tilde{\mathsf{E}}$, we will give the three queries for which we created an interdependency for free to the adversary. This can have any of three effects: (a) it increases the probability of a collision when the "bad" events do not occur; (b) it increases the probability of the "bad" events; or (c) it directly leads to a collision. By inspection, it can be seen that even in the worst case, the three free queries can only lead to a fixed number of additional bad configurations. Thus by changing the bound on the number of bad configurations, this case is taken care of. For (a) the probability increases slightly due to the changed bound on the bad events, but otherwise nothing of note changes. This leaves the investigation of (c). However, it is impossible that just the queries $(0^n|0^n, 0^n)$, $(0^n|0^n, c)$, and $(0^n|0^n, M_c)$ already lead to a collision, as jointly they determine at most one full TDM compression function evaluation. For neither $(0^n|0^n, c)$ nor for $(0^n|0^n, M_c)$ it is possible to occur on the lower half of Fig.(2.c) (since the corresponding upper-part query would have a key distinct from $0^n|0^n$ as both $c \neq 0$ and $M_c \neq 0$). Moreover, $(0^n|0^n, 0^n)$ can occur on the lower half, but it would only match with $\tilde{\mathsf{E}}^{-1}(0^n|0^n, 0^n)$. This could correspond to either of the free three queries (with very low probability), but never to several. Thus with some modifications (affecting tightness), the full Lee et al. proof goes through also for $\mathsf{TDM}^{\tilde{\mathsf{E}}}$. □

We now provide the remaining separations.

Theorem D.2 (Theorem 4.5, restated) *Let $c \in \{0,1\}^n \setminus \{0^n\}$. Then among the compression functions HDM_c, ADM, and TDM neither one directly reduces the idealized cipher in either one of the other two functions for the collision-resistance game.*

Proof. Let us start by separating Abreast-DM from the other two DBL compression functions. For a blockcipher E, define the modified blockcipher $\tilde{\mathsf{E}}$ as follows.

$$M_1 := \mathsf{E}^{-1}(1^n|0^n, \mathsf{E}(0^n|1^n, 0^n) \oplus 1^n)\,, \quad C_0 := \mathsf{E}(0^n|1^n, 0^n)\,, \quad C_1 := \mathsf{E}(1^n|0^n, 1^n)\,.$$

$$\tilde{\mathsf{E}}(K_1|K_2, M) := \begin{cases} C_0 \oplus 1^n & \text{if } (K_1|K_2, M) = (1^n|0^n, 1^n)\,; \\ C_1 & \text{if } (K_1|K_2, M) = (1^n|0^n, M_1)\,; \\ \mathsf{E}(K_1|K_2, M) & \text{otherwise.} \end{cases}$$

$$\tilde{\mathsf{E}}^{-1}(K_1|K_2, C) := \begin{cases} 1^n & \text{if } (K_1|K_2, C) = (1^n|0^n, C_0 \oplus 1^n)\,; \\ M_1 & \text{if } (K_1|K_2, C) = (1^n|0^n, C_1)\,; \\ \mathsf{E}^{-1}(K_1|K_2, C) & \text{otherwise.} \end{cases}$$

Note that $\tilde{\mathsf{E}}$ and $\tilde{\mathsf{E}}^{-1}$ as above define a blockcipher. We have

$$\mathsf{ADM}^{\tilde{\mathsf{E}}}(0^n, 0^n, 1^n) = (\tilde{\mathsf{E}}(0^n|1^n, 0^n) \oplus 0^n, \tilde{\mathsf{E}}(1^n|0^n, 1^n) \oplus 0^n) = (C_0, C_0 \oplus 1^n)\,,$$
$$\mathsf{ADM}^{\tilde{\mathsf{E}}}(1^n, 1^n, 0^n) = (\tilde{\mathsf{E}}(1^n|0^n, 1^n) \oplus 1^n, \tilde{\mathsf{E}}(0^n|1^n, 0^n) \oplus 1^n) = (C_0 \oplus 1^n \oplus 1^n, C_0 \oplus 1^n) = (C_0, C_0 \oplus 1^n)\,.$$

[5] We stress that this statement should not be taken as a conditional probability.

Hence the pair $((0^n, 0^n, 1^n), (1^n, 1^n, 0^n))$ constitutes a collision for ADM with respect to $\tilde{\mathsf{E}}$. Using a case analysis as in Lemma 4.4, it is possible to prove that for $\tilde{\mathsf{E}}$ a blockcipher as above, with $(\mathsf{E}, \mathsf{E}^{-1}) \leftarrow\!\!\$\ \mathsf{Block}(2n, n)$, the $\mathsf{TDM}^{\tilde{\mathsf{E}}}$ and $\mathsf{HDM}^{\tilde{\mathsf{E}}}_{1^n}$ compression functions are both collision resistant.

We now turn to Tandem-DM. Let E be a blockcipher. For this separation it is easier to derive the separation by tweaking the cipher at two points. This is due to the nested call that the TDM compression function places to E. Set

$$M_0 := \mathsf{E}^{-1}(0^n|0^n, 0^n)\,, \quad M_1 := \mathsf{E}^{-1}(1^n|1^n, 1^n)\,, \quad C_0 := \mathsf{E}(0^n|0^n, 0^n)\,, \quad \text{and} \quad C_1 := \mathsf{E}(1^n|1^n, 1^n)\,.$$

Now define a modified blockcipher $\tilde{\mathsf{E}}$ as follows.

$$\tilde{\mathsf{E}}(K_1|K_2, M) := \begin{cases} 0^n & \text{if } (K_1|K_2, M) = (0^n|0^n, 0^n)\,; \\ 1^n & \text{if } (K_1|K_2, M) = (1^n|1^n, 1^n)\,; \\ C_0 & \text{if } (K_1|K_2, M) = (0^n|0^n, M_0)\,; \\ C_1 & \text{if } (K_1|K_2, M) = (1^n|1^n, M_1)\,; \\ \mathsf{E}(K_1|K_2, M) & \text{otherwise.} \end{cases}$$

$$\tilde{\mathsf{E}}^{-1}(K_1|K_2, C) := \begin{cases} 0^n & \text{if } (K_1|K_2, C) = (0^n|0^n, 0^n)\,; \\ 1^n & \text{if } (K_1|K_2, C) = (1^n|1^n, 1^n)\,; \\ M_0 & \text{if } (K_1|K_2, C) = (0^n|0^n, C_0)\,; \\ M_1 & \text{if } (K_1|K_2, C) = (1^n|1^n, C_1)\,; \\ \mathsf{E}^{-1}(K_1|K_2, C) & \text{otherwise.} \end{cases}$$

Note that $\tilde{\mathsf{E}}$ and $\tilde{\mathsf{E}}^{-1}$ as above define a blockcipher. We have

$$\mathsf{TDM}^{\tilde{\mathsf{E}}}(0^n, 0^n, 0^n) = (\tilde{\mathsf{E}}(0^n|0^n, 0^n) \oplus 0^n, \tilde{\mathsf{E}}(0^n|0^n, 0^n) \oplus 0^n) = (0^n \oplus 0^n, 0^n \oplus 0^n) = (0^n, 0^n)\,,$$
$$\mathsf{TDM}^{\tilde{\mathsf{E}}}(1^n, 1^n, 1^n) = (\tilde{\mathsf{E}}(1^n|1^n, 1^n) \oplus 1^n, \tilde{\mathsf{E}}(1^n|1^n, 1^n) \oplus 1^n) = (1^n \oplus 1^n, 1^n \oplus 1^n) = (0^n, 0^n)\,.$$

Hence the pair $((0^n, 0^n, 0^n), (1^n, 1^n, 1^n))$ constitutes a collision for TDM with respect to $\tilde{\mathsf{E}}$. Using a case analysis as in Lemma 4.4, it is possible to prove that for $\tilde{\mathsf{E}}$ a blockcipher as above, with $(\mathsf{E}, \mathsf{E}^{-1}) \leftarrow\!\!\$\ \mathsf{Block}(2n, n)$, the $\mathsf{HDM}^{\tilde{\mathsf{E}}}_{1^n}$ and $\mathsf{ADM}^{\tilde{\mathsf{E}}}$ compression functions are both collision resistant. □

E Proof of Theorem 4.6: Irreducibility of PGV to DBL

Theorem E.1 (Theorem 4.6, restated) *There is no single-query fully black-box ideal-cipher reduction from any of the PGV constructions to any of the DBL constructions for the collision-resistance and [everywhere] preimage-resistance games as long as the reduction is tight: when the number of queries, run times, and success probabilities are parameterized by a security parameter, the reduction is $(\mathcal{O}(1), \mathcal{O}(1), \mathcal{O}(1), \mathcal{O}(1))$-tight.*

Let us first recall the precise concrete security bounds for the DBL constructions. We set $N := 2^n$ and $\mathcal{E}$ to be the uniform distribution on $\mathsf{Block}(2n, n)$ throughout. The bounds for Hirose-DM are

$$\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{HDM}_c, \mathcal{E}}(q) \le \frac{2q^2}{(N-2q)^2} + \frac{2q}{N-2q}\,,$$
$$\mathbf{Adv}^{\mathsf{pre}}_{\mathsf{HDM}_c, \mathcal{E}}(q) \le \frac{8q}{N^2} + \frac{8q}{N(N-2)}\,,$$
$$\mathbf{Adv}^{\mathsf{epre}}_{\mathsf{HDM}, \mathcal{E}}(q) \le \frac{8q}{N^2} + \frac{8q}{N(N-2)}\,,$$

where the collision-resistance bound holds for $2q < N$ and is from [FGL09b], and the [everywhere] preimage-resistance bounds are from [AFK+11] and are valid for any number of queries.

For Abreast-DM, when $q < N/6$, we have [LK11]

$$\begin{aligned}
\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{ADM},\mathcal{E}}(q) &\leq \frac{q}{(N-6q)} + \frac{18q^2}{(N-6q)^2}\,,\\
\mathbf{Adv}^{\mathsf{pre}}_{\mathsf{ADM},\mathcal{E}}(q) &\leq \frac{6q}{(N-6q)^2}\,,\\
\mathbf{Adv}^{\mathsf{epre}}_{\mathsf{ADM},\mathcal{E}}(q) &\leq \frac{6q}{(N-6q)^2}\,.
\end{aligned}$$

Finally, for Tandem-DM we have

$$\begin{aligned}
\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{TDM},\mathcal{E}}(q) &\leq 2N\left(\frac{2eq}{\alpha(N-2q)}\right)^{\alpha} + \frac{4q\alpha}{N-2q} + \frac{4q}{N-2q} \quad \text{for any} \quad 1 \leq \alpha \leq 2q < N,\\
\mathbf{Adv}^{\mathsf{pre}}_{\mathsf{TDM},\mathcal{E}}(q) &\leq \frac{16\alpha}{N} + \frac{8q}{N^2(N-2)} + 2\left(\frac{2eq}{\alpha N}\right)^{\alpha} + \frac{4q}{\alpha N} + \frac{q}{N^2(N-q)} \quad \text{for any} \quad 1 \leq \alpha \leq q < N,\\
\mathbf{Adv}^{\mathsf{epre}}_{\mathsf{TDM},\mathcal{E}}(q) &\leq \frac{16\alpha}{N} + \frac{8q}{N^2(N-2)} + 2\left(\frac{2eq}{\alpha N}\right)^{\alpha} + \frac{4q}{\alpha N} + \frac{q}{N^2(N-q)} + \frac{1}{N} \quad \text{for any} \quad 1 \leq \alpha \leq q < N,
\end{aligned}$$

where the collision-resistance bound is from [LSS11], and the [everywhere] preimage-resistance bound is taken from [AFK+11].

Proof. We only need to consider the reducibility of one of the PGV constructions as they reduce to each other via free transformations by Propositions 3.1 and 3.3.

Collision resistance. We start by treating the collision-resistance game. Let $\mathsf{DBL}^{\mathsf{E}}$ be a DBL construction with $(\mathsf{E}, \mathsf{E}^{-1})$ sampled from the ideal cipher $\mathcal{E}$. Suppose we have a fully black-box reduction $(\mathcal{T}, \mathcal{R})$ where $\mathcal{R}$ succeeds in outputting a collision for $\mathsf{DBL}^{\mathsf{E}}$ with constant probability ϵ_{coll} whenever it is provided with a collision for $\mathsf{PGV}_1^{\mathcal{T}^{\mathsf{E}}}$ from $\mathcal{B}$. From $\mathcal{R}$ we construct an algorithm $\mathcal{A}$ which runs the reduction, simulating $\mathcal{B}$, and breaks the collision resistance of $\mathsf{DBL}^{\mathsf{E}}$ with a probability exceeding its best security bound. This leads to a contradiction if the number of queries that $\mathcal{A}$ makes is within the range for which the bound applies. We show this is indeed the case as long as $\mathcal{R}$ does not place "too many" queries.

We derive $\mathcal{A}$ by letting it simulate a PGV collision-finder $\mathcal{B}$ for the reduction as follows. The reduction has access to blockcipher oracles $\mathsf{E}, \mathsf{E}^{-1}$ against which $\mathcal{A}$ also plays, but the reduction may nonetheless decide to provide $\mathcal{T}$ and $\mathcal{B}$ with simulated oracles $\tilde{\mathsf{E}}, \tilde{\mathsf{E}}^{-1}$. Hence, we consider an adversary $\mathcal{A}^{\mathsf{E},\mathsf{E}^{-1}}$ against $\mathsf{DBL}^{\mathsf{E}}$ which runs

$$\mathcal{R}^{\mathcal{B}^{\mathcal{T}^{\tilde{\mathsf{E}},\tilde{\mathsf{E}}^{-1}},\mathcal{T}^{-1^{\tilde{\mathsf{E}},\tilde{\mathsf{E}}^{-1}}}},\mathsf{E},\mathsf{E}^{-1}}$$

and answers $\mathcal{R}$'s queries to E and E^{-1} using its own oracles. The reduction's single query to the (black-box) adversarial interface $\mathcal{B}$ is answered as follows. $\mathcal{A}$ computes $q_{\mathcal{A}}$ values of PGV_1 (for a $q_{\mathcal{A}}$ to be determined later on) with respect to $\mathcal{T}^{\tilde{\mathsf{E}},\tilde{\mathsf{E}}^{-1}}$. To this end, $\mathcal{A}$ needs to run $\mathcal{T}$ and answer its blockcipher queries. Note that the reduction $\mathcal{R}$ may be *programming* the blockcipher and $\mathcal{A}$ cannot simply answer $\mathcal{T}$'s queries by forwarding them to its own oracles. Algorithm $\mathcal{A}$ handles these queries through $\mathcal{R}$. Assuming the reduction places at most q_{E} queries to E or E^{-1} for each blockcipher query of $\mathcal{T}$, and that $\mathcal{T}$ places at most $q_{\mathcal{T}}$ queries to its oracles for each evaluation, we get that $\mathcal{A}$ makes a total of at most $q_{\mathsf{E}} \cdot q_{\mathcal{T}} \cdot q_{\mathcal{A}}$ queries to E or E^{-1} at this stage. Once the $q_{\mathcal{A}}$ values are computed, if $\mathcal{A}$ finds a collision, it returns it. Else it returns a pair of random distinct points. Algorithm $\mathcal{A}$ resumes $\mathcal{R}$ as before, and terminates by outputting whatever $\mathcal{R}$ outputs. Assuming that $\mathcal{R}$ places at most $q_{\mathcal{R}}$ queries to E or E^{-1} (in addition

to those for handling $\mathcal{T}$'s queries), we have that algorithm $\mathcal{A}$ makes a total of at most $q_{\mathsf{Tot}} := q_{\mathcal{R}} + q_{\mathsf{E}} \cdot q_{\mathcal{T}} \cdot q_{\mathcal{A}}$ queries to E or E^{-1} during its run.

Using the results of Bellare and Kohno that the lower bound for the generic on the collision resistance of a compression function can only increase if the function is not "balanced" [BK04], we know that for *any* given blockcipher E', the lower bound on the success probability of the attack on the collision resistance of $\mathsf{PGV}_1^{\mathsf{E}'}$ (as given in Section 3) applies. Hence *independently of the specification of* $\mathcal{T}$ we have

$$\begin{aligned}
\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{DBL},\mathcal{E}}(q_{\mathsf{Tot}}) &\geq \mathbf{Adv}^{\mathsf{coll}}_{\mathsf{DBL},\mathcal{E}}(\mathcal{A}) \\
&= \Pr\left[\mathcal{A} \text{ finds a } \mathsf{DBL}^{\mathsf{E}} \text{ collision}\right] \\
&\geq \Pr\left[\mathcal{R} \text{ finds a } \mathsf{DBL}^{\mathsf{E}} \text{ coll.} \mid \mathcal{A} \text{ finds a } \mathsf{PGV}_1^{\mathcal{T}^{\mathsf{E},\mathsf{E}^{-1}}} \text{ coll.}\right] \cdot \Pr\left[\mathcal{A} \text{ finds a } \mathsf{PGV}_1^{\mathcal{T}^{\mathsf{E},\mathsf{E}^{-1}}} \text{ coll.}\right] \\
&\geq \epsilon_{\mathsf{coll}} \cdot \frac{1}{8e} \frac{q_{\mathcal{A}}^2 + 1}{N} \,.
\end{aligned}$$

Let us now consider the above inequality for Hirose-DM. In order to simplify the analysis we use the simpler $6q/N$ upper bound for the collision-resistance advantage when $q \leq N/4$. Setting $\epsilon := \epsilon_{\mathsf{coll}}/(6 \cdot 8e)$, we get

$$\epsilon \cdot \frac{q_{\mathcal{A}}^2 + 1}{N} \leq \frac{q_{\mathcal{R}} + q_{\mathsf{E}} \cdot q_{\mathcal{T}} \cdot q_{\mathcal{A}}}{N} \,,$$

which implies

$$q_{\mathcal{A}} \leq \frac{1}{2\epsilon}\left(q_{\mathsf{E}} q_{\mathcal{T}} + \sqrt{q_{\mathsf{E}}^2 q_{\mathcal{T}}^2 + 4\epsilon q_{\mathcal{R}} - 4\epsilon^2}\right) \leq \frac{1}{\epsilon}\left(q_{\mathsf{E}} q_{\mathcal{T}} + \sqrt{\epsilon q_{\mathcal{R}}}\right) .$$

We obtain the desired contradiction if $q_{\mathcal{A}}$ can be chosen so that it is larger than the upper bound given above while ensuring that the total number of queries falls within the range for which the collision-resistance bound holds, i.e., when $q_{\mathsf{Tot}} \leq N/4$. In order to show that these constraints can be met, we need to have that

$$\frac{1}{\epsilon}\left(q_{\mathsf{E}} q_{\mathcal{T}} + \sqrt{\epsilon q_{\mathcal{R}}}\right) + 1 \leq q_{\mathcal{A}} \leq \frac{N/4 - q_{\mathcal{R}}}{q_{\mathsf{E}} q_{\mathcal{T}}} \,.$$

This is the case if

$$q^4 + q^2\sqrt{2\epsilon q} + \epsilon q^2 + \epsilon q \leq \epsilon N/4 \,,$$

where $q := \max\{q_{\mathcal{R}}, q_{\mathsf{E}}, q_{\mathcal{T}}\}$. Whenever $q \leq c \cdot \sqrt[4]{\epsilon_{\mathsf{coll}} N}$, for a constant $c \approx 6.75$, one can always pick a $q_{\mathcal{A}}$ such that it meets the above constraints. Hence reductions satisfying this inequality for q (e.g., those which are tight) are ruled out.

The collision-resistance irreducibility proofs for Abreast-DM and Tandem-DM are similar to that for Hirose-DM. The main difference is that we arrive at different constraints for $q_{\mathcal{A}}$.

For Abreast-DM, we may simplify the collision-resistance bound to $8q/N$ when $q \leq N/12$. Setting $\epsilon := \epsilon_{\mathsf{coll}}/(8 \cdot 8e)$ we get

$$\epsilon \cdot \frac{q_{\mathcal{A}}^2 + 1}{N} \leq \frac{q_{\mathcal{R}} + q_{\mathsf{E}} \cdot q_{\mathcal{T}} \cdot q_{\mathcal{A}}}{N} \,.$$

This inequality is identical to that derived for Hirose-DM (except that the constant ϵ has a different value), and the rest of the analysis follows that for Hirose-DM.

For Tandem-DM we set $\alpha = 3$. This ensures that the collision-resistance bound grows more slowly than q^2/N. (Note that this is not the case when $\alpha \leq 2$.) With this choice of α (and noting that $e < 3$) we obtain the simpler bound

$$\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{TDM},\mathcal{E}}(q) \leq \frac{16Nq^3}{(N-2q)^3} + \frac{16q}{N-2q} \leq \frac{128q^3}{N^2} + \frac{32q}{N} \leq \frac{40q}{N} \,,$$

where the penultimate and final inequalities holds for $q \leq N/4$ and $q \leq \sqrt{N}/4$ respectively. Setting $\epsilon := \epsilon_{\mathsf{coll}}/(40 \cdot 8e)$ we get

$$\epsilon \cdot \frac{q_{\mathcal{A}}^2 + 1}{N} \leq \frac{q_{\mathcal{R}} + q_{\mathsf{E}} \cdot q_{\mathcal{T}} \cdot q_{\mathcal{A}}}{N} .$$

Continuing with the analysis as in Hirose-DM we finally arrive at

$$q^4 + q^2\sqrt{2\epsilon q} + \epsilon q^2 + \epsilon q \leq \epsilon\sqrt{N}/4 ,$$

where $q := \max\{q_{\mathcal{R}}, q_{\mathsf{E}}, q_{\mathcal{T}}\}$ as before. Therefore reductions for which $q \leq c \cdot \sqrt[8]{\epsilon_{\mathsf{coll}}^2 N}$, for some constant c, are ruled out.

[Everywhere] preimage resistance. The intuition behind the proofs for the [everywhere] preimage-resistance games for HDM, ADM, and TDM are as in the collision-resistance games. The proof will utilize theorems analogous to that of Bellare and Kohno [BK04] for the [everywhere] preimage-resistance game. Algorithm $\mathcal{A}$ in the analysis is modified to output a random domain point if it does not find a preimage among its $q_{\mathcal{A}}$ queries. Therefore, the lower bound corresponding to the success probability of $\mathcal{A}$ against PGV_1 for the [everywhere] preimage-resistance game, independently of $\mathcal{T}$, is $\epsilon_{\mathsf{pre}}(q_{\mathcal{A}} + 1)/(2N)$. We now treat each DBL compression function.

For Hirose-DM we use the simplified $32q/N^2$ bound for [everywhere] preimage resistance when $N \geq 3$. (This can be derived from the more precise bound given in Section 4.3.) Setting $\epsilon := \epsilon_{\mathsf{pre}}/(2 \cdot 32)$ we get

$$\epsilon \cdot \frac{q_{\mathcal{A}} + 1}{N} \leq \frac{q_{\mathcal{R}} + q_{\mathsf{E}} \cdot q_{\mathcal{T}} \cdot q_{\mathcal{A}}}{N^2} .$$

It is enough to consider this inequality for $q_{\mathcal{A}} = 0$. In this case we get that $q_{\mathcal{R}} \geq \epsilon N$, and since ϵ_{pre} (and hence ϵ) is a constant, the reduction must be placing a large number of queries, and cannot be tight. The analysis for the everywhere preimage-resistance game is identical.

For Abreast-DM we simplify the [everywhere] preimage-resistance bound to $24q/N^2$ for $q \leq N/12$. Setting $\epsilon := \epsilon_{\mathsf{pre}}/(2 \cdot 24)$ we get

$$\epsilon \cdot \frac{q_{\mathcal{A}} + 1}{N} \leq \frac{q_{\mathcal{R}} + q_{\mathsf{E}} \cdot q_{\mathcal{T}} \cdot q_{\mathcal{A}}}{N^2} .$$

Once again, for $q_{\mathcal{A}} = 0$ we must have that $q_{\mathcal{R}} \geq \epsilon N$, and the reduction cannot be tight. Everywhere preimage resistance is treated identically.

For Tandem-DM we treat the everywhere preimage-resistance game as the advantage bound for this game is higher than that for the preimage-resistance advantage by $1/N$. We set $\alpha = 2 + \sqrt{q}$ so that the advantage bound grows more slowly than q/N. (Note that a constant value for α is not sufficient to ensure this condition.) We have

$$\begin{aligned}
\mathbf{Adv}^{\mathsf{epre}}_{\mathsf{TDM},\mathcal{E}}(q) &\leq \frac{16(2+\sqrt{q})+1}{N} + \frac{4q}{N(2+\sqrt{q})} + 2\left(\frac{6^2q^2}{N^2(2+\sqrt{q})^2}\right)\left(\frac{6q}{N(2+\sqrt{q})}\right)^{\sqrt{q}} + \frac{q}{N^2(N-q)} + \frac{8q}{N^2(N-2)} \\
&\leq \frac{20\sqrt{q}}{N} + \frac{72q}{N^2} + \frac{2q}{N^3} + \frac{24q}{N^3} + \frac{33}{N} \quad \text{for} \quad q \leq N/2 \text{ and } N \geq 3 \\
&\leq \frac{151\sqrt{q}}{N} \quad \text{for} \quad q \geq 3 .
\end{aligned}$$

Setting $\epsilon := \epsilon_{\mathsf{pre}}/(2 \cdot 151)$ we finally arrive at

$$\epsilon \cdot \frac{q_{\mathcal{A}} + 1}{N} \leq \frac{\sqrt{q_{\mathcal{R}} + q_{\mathsf{E}} \cdot q_{\mathcal{T}} \cdot q_{\mathcal{A}}}}{N} , \quad \text{which implies} \quad q_{\mathcal{A}} \leq \frac{1}{\epsilon^2}(q_{\mathsf{E}} q_{\mathcal{T}} + \epsilon\sqrt{q_{\mathcal{R}}}) .$$

The rest of the analysis is similar to Hirose-DM: applying the bound on the total number of queries for which the above inequality holds we obtain

$$q^4 + \epsilon q^2 \sqrt{q} + \epsilon^2 q^2 + \epsilon^2 q \leq \epsilon^2 N/2\,,$$

where $q := \max\{q_{\mathcal{R}}, q_{\mathsf{E}}, q_{\mathcal{T}}\}$ as before. As a result reductions for which $q \leq c \cdot \sqrt[4]{\epsilon_{\mathsf{pre}}^2 N}$, for some constant c, are ruled out. □