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

Paul Baecher[1], Pooya Farshim[1], Marc Fischlin[1], and 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 functions 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 [27] 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

T. Johansson and P. Nguyen (Eds.): EUROCRYPT 2013, LNCS 7881, pp. 426–443, 2013.

SHA-3 competition, Skein [13], explicitly refers to this design methodology, and other former candidates like Grøstl [15] 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. [9,10]. 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 sub-optimal 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. [10], 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 [33], while for AES recent related-key attacks [7,8] cast some shadow on its suitability for this purpose. Indeed, Khovratovich [20, 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 [4] 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 [30]. Although we can ask the same question for indifferentiability from random functions [25], the PGV constructions, as pointed out in [11,21], 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. [27] 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 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

[1] This mainly motivates why we chose the oracle reducibility notion of [4] rather than the indifferentiability reducibility notion in [25].

functions, namely, Tandem-DM (TDM, [22]), Abreast-DM (ADM, [22]), and Hirose's construction (HDM, [19]). Several results underline the optimality of collision-resistance [19,23,24] and preimage-resistance bounds [2] for these functions in the ICM.

We next 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 [17,16,26]. 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 [26] 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 [26] with a lower bound on generic collision finders by Bellare and Kohno [5] 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 [26]). 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.

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 1 (Everywhere preimage and collision resistance [30]). *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*

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

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

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

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 [29].

Some of our results also hold for "more advanced" properties of hash or compression functions like preimage awareness [12]. (The definition can be found in the full version of the paper.) 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 [6]. 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 (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*

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

where the probability is taken over 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*

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

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 sub-game to play and then invoking the corresponding parties and game. Note also that as in [4] 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 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*

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

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*

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

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 [4] 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.

3 Reducibility among the PGV Functions

We start by recalling the blockcipher-based constructions of hash functions by Preneel et al. [27,10]. 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 $\{0,1\}^n$:

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

There are 64 basic combinations to build such a compression function, of which 12 were first believed [27] (under category "✓" or "FP") and later actually proven to be secure [10] (under category "group-1"). We denote these secure compression functions by $\mathsf{PGV}_1, \ldots, \mathsf{PGV}_{12}$ and adopt the s-index of [10] (as defined in Figure 2 there); they are depicted in Figure 1. The PGV_1 and PGV_5 functions can be instantiated with a blockcipher whose key length and message length are not equal. The remaining function, however, do not natively support this feature but they can be generalized such that they do [32].

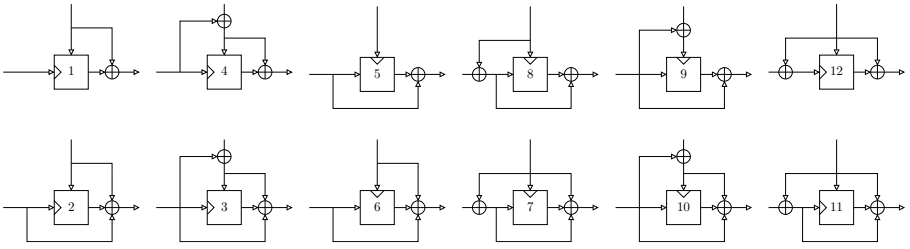


Fig. 1. The 12 optimally secure PGV constructions $\mathsf{PGV}_i^{\mathsf{E}}$ for $i \in [12]$. A triangle denotes the location of the key input. When used in an iteration mode, the top input is a message block and the left input is the chaining value. The first (resp. second) row corresponds to the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

For $i \in [12]$ and $q \geq 0$, the security bounds for uniform $\mathcal{E}$ according to [9,32,10] 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 [10][2]

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

$$\mathbf{Adv}^{\mathsf{epre}}_{\mathsf{PGV}_i,\mathcal{E}}(\mathcal{B}) \geq \frac{q+1}{2^{n+1}}\,.$$

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.

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

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. [27] 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 [12] to the games which are preserved.

Proposition 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.*

The proof of Proposition 1 appears in the full version of this paper.

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.

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

Theorem 1. *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 the full version of this paper.

Proposition 2. *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).*

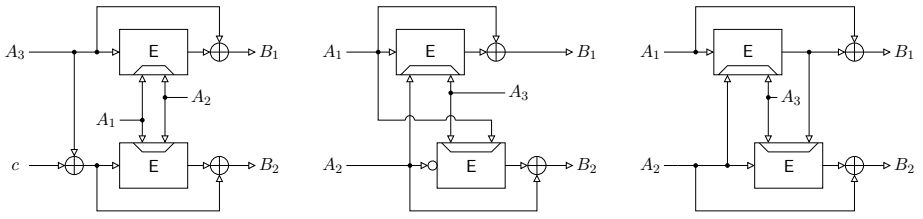
To prove this (which we do in the full version of this paper), we first show that there is a transformation such that there is an inter-group reduction, i.e., $\mathsf{PGV}_2 \in \mathcal{G}_2$ reduces to $\mathsf{PGV}_1 \in \mathcal{G}_1$ and vice versa—indeed we will use the same transformation for either direction. By transitivity we then obtain a reduction for any two constructions through Proposition 1, where we view the identity transformation as a special case of an arbitrary one.

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 [18,19], Abreast-DM [22,23], and Tandem-DM [22,24,14], 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

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



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

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

We denote the Hirose-DM for a constant $c \in \{0,1\}^n \backslash \{0^n\}$, 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).

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

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 3. *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.*

The proof of the proposition appears in the full version of this paper. 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 the full version.

Proposition 4. *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 5. *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.*

[3] There exist modifications of the PGV constructions which can be instantiated with DBL blockciphers [32]. We leave their treatment to future work.

For space reasons, we defer the proof to the full version of this paper.

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 [1], 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 3. 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 3 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.

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

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

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

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

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

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 the full version of this paper.

Lemma 1. *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 also provide the remaining separating examples in the full version of this paper.

Theorem 2. *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 3, 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 3 and 5: 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 [28]. 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 [28], 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 [3], 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 [26]. 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 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 the full version.

Theorem 3. *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 [26] 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 $\mathsf{HDM}^{\mathsf{E}^\star}_{1^n}$ but renders $\mathsf{ADM}^{\mathsf{E}^\star}$ collision-tractable (see the full version of this paper). 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 $\mathsf{HDM}^{\mathsf{E}}_{1^n}$ 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.

[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.

	$\mathcal{G}_1$	$\mathcal{G}_2$	TDM	HDM_c	ADM
$\mathcal{G}_1$	Y 1	N 1	Y 3	Y 3	Y 3
$\mathcal{G}_2$	N 1	Y 1	–	–	–
TDM	N 2	–	Y	N 2	N 2
HDM_c	N 2	–	N 2	Y	N 2
ADM	N 2	–	N 2	N 2	Y

(3.a) Results for the identity transformation.

	$\mathcal{G}_1$	$\mathcal{G}_2$	TDM	HDM_c	ADM
$\mathcal{G}_1$	Y $\rightarrow$	Y 2	Y $\rightarrow$	Y $\rightarrow$	Y $\rightarrow$
$\mathcal{G}_2$	Y 2	Y $\rightarrow$	Y $\star$	Y $\star$	Y $\star$
TDM	N 3	N 3	Y	n 2	n 2
HDM_c	N 3	N 3	n 2	Y	n 2
ADM	N 3	N 3	n 2	n 2	Y

(3.b) Results for arbitrary transformations.

Fig. 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.

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 [31] 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. We thank the anonymous reviewers for their valuable comments. 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

1. Andreeva, E., Neven, G., Preneel, B., Shrimpton, T.: Seven-property-preserving iterated hashing: ROX. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 130–146. Springer, Heidelberg (2007)
2. Armknecht, F., Fleischmann, E., Krause, M., Lee, J., Stam, M., Steinberger, J.: The preimage security of double-block-length compression functions. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 233–251. Springer, Heidelberg (2011)
3. Baecher, P., Brzuska, C., Fischlin, M.: Notions of black-box reductions, revisited. Cryptology ePrint Archive, Report 2013/101 (2013), `http://eprint.iacr.org/`
4. Baecher, P., Fischlin, M.: Random oracle reducibility. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 21–38. Springer, Heidelberg (2011)
5. Bellare, M., Kohno, T.: Hash function balance and its impact on birthday attacks. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 401–418. Springer, Heidelberg (2004)
6. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 409–426. Springer, Heidelberg (2006)
7. Biryukov, A., Khovratovich, D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 1–18. Springer, Heidelberg (2009)
8. Biryukov, A., Khovratovich, D., Nikolić, I.: Distinguisher and related-key attack on the full AES-256. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 231–249. Springer, Heidelberg (2009)
9. Black, J.A., Rogaway, P., Shrimpton, T.: Black-box analysis of the block-cipher-based hash-function constructions from PGV. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 320–335. Springer, Heidelberg (2002)

10. Black, J., Rogaway, P., Shrimpton, T., Stam, M.: An analysis of the blockcipher-based hash functions from PGV. Journal of Cryptology 23(4), 519–545 (2010)
11. Coron, J.-S., Dodis, Y., Malinaud, C., Puniya, P.: Merkle-damgård revisited: How to construct a hash function. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 430–448. Springer, Heidelberg (2005)
12. Dodis, Y., Ristenpart, T., Shrimpton, T.: Salvaging merkle-damgård for practical applications. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 371–388. Springer, Heidelberg (2009)
13. Ferguson, N., Lucks, S., Schneier, B., Whiting, D., Bellare, M., Kohno, T., Callas, J., Walker, J.: The skein hash function family (2008)
14. Fleischmann, E., Gorski, M., Lucks, S.: On the security of TANDEM-DM. In: Dunkelman, O. (ed.) FSE 2009. LNCS, vol. 5665, pp. 84–103. Springer, Heidelberg (2009)
15. Gauravaram, P., Knudsen, L.R., Matusiewicz, K., Mendel, F., Rechberger, C., Schläfffer, M., Thomsen, S.S.: Grøstl — a SHA-3 candidate (2011)
16. Harnik, D., Kilian, J., Naor, M., Reingold, O., Rosen, A.: On robust combiners for oblivious transfer and other primitives. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 96–113. Springer, Heidelberg (2005)
17. Herzberg, A.: On tolerant cryptographic constructions. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 172–190. Springer, Heidelberg (2005)
18. Hirose, S.: Provably secure double-block-length hash functions in a black-box model. In: Park, C.-S., Chee, S. (eds.) ICISC 2004. LNCS, vol. 3506, pp. 330–342. Springer, Heidelberg (2005)
19. Hirose, S.: Some plausible constructions of double-block-length hash functions. In: Robshaw, M. (ed.) FSE 2006. LNCS, vol. 4047, pp. 210–225. Springer, Heidelberg (2006)
20. Khovratovich, D.: New Approaches to the Cryptanalysis of Symmetric Primitives. Ph.D. thesis, University of Luxembourg (2010)
21. Kuwakado, H., Morii, M.: Indifferentiability of single-block-length and rate-1 compression functions. IEICE Transactions 90-A(10), 2301–2308 (2007)
22. Lai, X., Massey, J.L.: Hash functions based on block ciphers. In: Rueppel, R.A. (ed.) EUROCRYPT 1992. LNCS, vol. 658, pp. 55–70. Springer, Heidelberg (1993)
23. Lee, J., Kwon, D.: The security of abreast-dm in the ideal cipher model. IEICE Transactions 94-A(1), 104–109 (2011)
24. Lee, J., Stam, M., Steinberger, J.: The collision security of tandem-DM in the ideal cipher model. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 561–577. Springer, Heidelberg (2011)
25. Maurer, U.M., Renner, R.S., Holenstein, C.: Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 21–39. Springer, Heidelberg (2004)
26. Pietrzak, K.: Compression from collisions, or why CRHF combiners have a long output. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 413–432. Springer, Heidelberg (2008)
27. Preneel, B., Govaerts, R., Vandewalle, J.: Hash functions based on block ciphers: A synthetic approach. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 368–378. Springer, Heidelberg (1994)
28. Reingold, O., Trevisan, L., Vadhan, S.P.: Notions of reducibility between cryptographic primitives. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 1–20. Springer, Heidelberg (2004)
29. Rogaway, P.: Formalizing human ignorance. In: Nguyen, P.Q. (ed.) VIETCRYPT 2006. LNCS, vol. 4341, pp. 211–228. Springer, Heidelberg (2006)

30. Rogaway, P., Shrimpton, T.: Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In: Roy, B., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 371–388. Springer, Heidelberg (2004)
31. Simon, D.R.: Findings collisions on a one-way street: Can secure hash functions be based on general assumptions? In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 334–345. Springer, Heidelberg (1998)
32. Stam, M.: Blockcipher-based hashing revisited. In: Dunkelman, O. (ed.) FSE 2009. LNCS, vol. 5665, pp. 67–83. Springer, Heidelberg (2009)
33. Wei, L., Peyrin, T., Sokołowski, P., Ling, S., Pieprzyk, J., Wang, H.: On the (In)Security of IDEA in various hashing modes. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 163–179. Springer, Heidelberg (2012)