Design Rationality and Security Analysis of PHC Candidates: Overview

Dmitry Khovratovich

University of Luxembourg

dmitry.khovratovich@uni.lu

October 2, 2014

1 Introduction

The PHC call for submissions explicitly stated the following goals, among others:

- Cryptographic security;
- Lack of speed-up or other efficiency improvement (in terms of memory usage or area-time product per password) of cracking-optimized implementations on various platforms;
- Overall clarity of the scheme.

These goals follow clearly from the letter and spirit of previous cryptographic competitions: AES, eSTREAM, SHA-3, etc., on which the PHC is also explicitly based.

Whereas the first two goals are less subject to discussion, the clarity of the scheme and, speaking more generally, design rationale is often overlooked by the designers. Let us first cite the relevant statements from the previous competitions:

- *The submission of all design rationale is strongly encouraged, in order to facilitate the public evaluation process.* — AES call for submissions.
- *[Submission must provide] a design rationale explaining design choices.* — eSTREAM call for submissions.
- *"The document shall include design rationale (e.g., the rationale for choosing the specific number of rounds for computing the hashes) and an explanation for all the important design decisions that are made."* — SHA-3 call for submissions.

Apart from the explicitly mentioned reason to facilitate the evaluation process, the design rationale should also do the following:

- Inspire confidence in the design strength. In other words, the community of users and analysts should realize that the design decisions are sound, that the designer has chosen the components to maximize the security or at least not lower it, that the designer tried other possible solutions and has taken the best one.
- Convince in the absence of trapdoors or other deliberately injected weaknesses. Trapdoors may be hidden everywhere: from the scheme structure to internal constants. Clearly, it is much easier to hide a weakness in a more sophisticated design: the more components we have, the more combinations exist that may fail under certain circumstances. It is also easier to make mistakes and overlook them.

All these reasons are clearly related to the overall security of the design, and not that much to the performance issues.

Security analysis. Initial security analysis according to the goals called by PHC might be also considered a part of the design rationale. Trying to attack their own scheme, the designers not only detect weaknesses at the early stage, but also reduce the workload for future cryptanalysts. The absence of such attacks in the design document signals of little time devoted to analyze the own submission.

	Design complexity	Single phase	Single variant	Choices explained		
				Components	Mode of operation	Memory access pattern
Antcrypt	Low	Yes	Yes	Partly	Partly	No
Argon	Moderate	Yes	Yes	Yes	Yes	Yes
Battcrypt	Low	Yes	No	Yes	Partly	Yes
Catena	Low	Yes	Yes	Yes	Yes	Yes
Centrifuge	Moderate	No	Yes	No	No	No
Earworm	Moderate	No	No	Yes	No	No
Gambit	Low	Yes	Yes	No	No	No
Lanarea	Low	No	Yes	No	No	No
Lyra2	Moderate	No	Yes	Yes	Partly	Yes
Makwa	Low	No	Yes	Yes	Yes	N/A
MCS_PHS	Low	Yes	Yes	No	No	No
OmegaCrypt	Low	Yes	Yes	No	Partly	No
Parallel	Low	Yes	Yes	No	No	No
Pomelo	Moderate	No	Yes	No	No	No
Pufferfish	Moderate	Yes	Yes	No	No	No
Rig	Low	Yes	Yes	Yes	No	No
Schvrch	Moderate	No	Yes	No	No	No
Tortuga	Low	Yes	Yes	No	No	No
TwoCats	High	No	No	Partly	Partly	Partly
Yarn	Low	Yes	Yes	No	No	No
Yescrypt	High	No	No	Partly	Yes	Yes

Table 1: Design rationale of PHC candidates.

2 Survey

We exclude the withdrawn candidates and PolyPassHash from the comparison. We take the submission document as the primary source for the design decisions.

The summary of design rationale is given in Table 1. We introduced three categories: Low, Moderate, and High, and measured the candidates by the overall clarity and ease of understanding of the design (Design Complexity parameter). If the scheme uses two or more different phases (e.g., it is a hybrid design to defeat timing attacks), which have to be cryptanalyzed separately, we mark it as having *multiple phases*. If the scheme uses several parameters/flags, which modify the properties significantly, we mark it as having *multiple variants*, since all the variants also have to be analyzed separately. Finally, we check the motivation behind the overall mode of operation (i.e. the scheme data flow), designing internal components (if they are ad-hoc constructions or some reduced versions of existing functions), and the memory access pattern (which is supposed to ensure memory-hardness).

The summary of the security analysis is given in Table 2. An ideal candidate would have "Explored" or "N/A" in all columns, as these values demonstrate that particular properties have been investigated in details and the relevant attacks are well understood or just do not apply. "Attacked" implies that some vulnerabilities were revealed by the third-party analysis, which makes the discovery of new attacks more likely. When the submission does not analyze the tradeoff resilience, but we suspect that it could suffer to the tradeoff attacks shown for Catena and Lyra, we mark it as "Possible".

	Basic cryptography	Tradeoff analysis	GPU defense	FPGA/ASIC defense	Timing attacks
Antcrypt	Claimed	-	-	-	Possible
Argon	Explored	Explored	Claimed	Explored	Possible
Battcrypt	Claimed	-	Claimed	-	Possible
Catena	Explored	Attacked	Claimed	Attacked	N/A
Centrifuge	-	Possible	Claimed	Claimed	-
Earworm	Violated	Claimed	Claimed	Claimed	Explored
Gambit	Proven	Explored/Possible	-	-	N/A
Lanarea	Claimed	-	Claimed	Claimed	Possible
Lyra2	Claimed	Attacked	Explored	Attacked	Possible
Makwa	Proven	N/A	Possible	Possible	Explored
MCS_PHS	Claimed	Possible	-	-	-
OmegaCrypt	Claimed	-	-	-	Attacked
Parallel	Claimed	-	Claimed	Claimed	-
Pomelo	Claimed	Possible	Claimed	-	N/A
Pufferfish	Claimed	-	Claimed	-	Possible
Rig	Claimed	Explored/Possible	-	-	N/A
Schvrch	Claimed	Damaged	-	-	Possible
Tortuga	Claimed	Possible	-	-	-
TwoCats	Claimed	Explored/Possible	Claimed	Claimed	Possible
Yarn	Claimed	Claimed	Claimed	Claimed	Possible
Yescrypt	Claimed	Explored	Claimed	Claimed	Possible

Table 2: Security analysis of PHC candidates.
Legend:

- *Basic cryptography* — collision/preimage resistance, unpredictability.
- *Claimed* — security stated without deep investigation.
- *Explored* — security investigated by authors with some details, potential attacks present.
- *Proven* — security proven by reduction to the security of the underlying primitive.
- *Possible* — attacks seem possible: data-dependent branching/access for timing attacks, fixed memory access for tradeoff implementations.
- *Attacked* — third-party attacks better than projected by the designers or violating the security claims.
- *N/A* — attacks not applicable due to scheme structure.
- *Violated* — security property does not hold by design.
- - — no analysis by any party.