Erratum

Mikhail Anokhin*

Constructing a pseudo-free family of finite computational groups under the general integer factoring intractability assumption

https://doi.org/10.1515/gcc-2019-2009
Received April 20, 2019

Erratum to: M. Anokhin, Constructing a pseudo-free family of finite computational groups under the general integer factoring intractability assumption, Groups Complex. Cryptol. 5 (2013), no. 1, 53–74 (https://doi.org/10.1515/gcc-2013-0003).

Abstract: We provide a correct version of Remark 3.5 of the paper mentioned in the title. Also, we fix a typo in Remark 4.4 of that paper.

Keywords: Computational group, pseudo-free family of finite computational groups, general integer factoring intractability assumption, variety of groups

MSC 2010: 68Q17, 11Y05, 20E10, 94A60

In [1, Remark 3.5], we construct (under certain additional assumptions) a collision-intractable hash function family from a pseudo-free family of finite computational groups in a nontrivial variety of groups. However, that construction is incorrect. Moreover, the following assumption made in [1, Remark 3.5] is redundant: For each $d \in \operatorname{supp} \mathcal{D}_k$ $(k \in K)$, ρ_d is one-to-one.

Until now, to the best of our knowledge, there are no works using Remark 3.5 of [1] in the proofs. Therefore the error in that remark has not yet affected the validity of other results.

Here is a correct version of Remark 3.5 of [1]. In this version, we construct a collision-intractable hash function family in a slightly more general sense than in the original version.

Remark 3.5. Assume that the family of computational groups $((G_d, \rho_d, \mathcal{R}_d) \mid d \in D)$ is pseudo-free in $\mathfrak{V}$ with respect to $\mathcal{D}$ and σ. In this remark, we need the following additional assumptions:

- The variety $\mathfrak{V}$ is nontrivial (as in Remark 3.4).
- There exists a deterministic polynomial-time algorithm that, given integers $b_1, \dots, b_m \in \{0, 1\}$, computes $[a_1^{b_1} \dots a_m^{b_m}]_\sigma$ (as in Remark 3.4).
- There exists a polynomial η such that $\operatorname{dom} \rho_d \subseteq \{0, 1\}^{\eta(k)}$ for all $k \in K$ and $d \in \operatorname{supp} \mathcal{D}_k$.

Let π be a polynomial such that $\pi(k) > \eta(k)$ for any $k \in K$. Suppose $k \in K$. Denote by W_k the set of all pairs $(d, (r_1, \dots, r_{\pi(k)}))$ such that $d \in \operatorname{supp} \mathcal{D}_k$ and $r_1, \dots, r_{\pi(k)} \in \operatorname{dom} \rho_d$. For every $w \in W_k$, let $\psi_{k,w}$ be a mapping defined as in Remark 3.4. Moreover, we choose these mappings so that, given $(1^k, w)$ (where $w \in W_k$) and $y \in \{0, 1\}^{\pi(k)}$, $\psi_{k,w}(y)$ can be computed in deterministic polynomial time. Also, suppose $\mathcal{W}_k$ is the distribution of the random variable $(\mathbf{d}, (\mathbf{r}_1, \dots, \mathbf{r}_{\pi(k)}))$, where $\mathbf{d} \leftarrow \mathcal{D}_k$ and $\mathbf{r}_1, \dots, \mathbf{r}_{\pi(k)} \leftarrow \mathcal{R}_{\mathbf{d}}$. Of course, the probability ensemble $(\mathcal{W}_k \mid k \in K)$ is polynomial-time samplable. Then Remark 3.4 implies that the family $(\psi_{k,w} \mid k \in K, w \in W_k)$ is a collision-intractable (or collision-resistant) hash function family with respect

***Corresponding author: Mikhail Anokhin,** Information Security Institute, Lomonosov University, Moscow, Russia, e-mail: anokhin@mccme.ru. http://orcid.org/0000-0002-3960-3867

to $(\mathcal{W}_k \mid k \in K)$. Namely, the following conditions hold:

- For all $k \in K$ and $w \in W_k$, $\psi_{k,w}$ maps $\{0,1\}^{\pi(k)}$ into $\{0,1\}^{\eta(k)}$, where $\pi(k) > \eta(k)$.
- Given $(1^k, w)$ (where $k \in K$ and $w \in W_k$) and $y \in \{0,1\}^{\pi(k)}$, $\psi_{k,w}(y)$ can be computed in deterministic polynomial time.
- If $\mathbf{w} \leftarrow \mathcal{W}_k$, then for any probabilistic polynomial-time algorithm A,

$$\Pr(A(1^k, \mathbf{w}) \text{ is a collision for } \psi_{k,\mathbf{w}})$$

  is negligible as a function of $k \in K$.

In fact, this remark (as well as [1, Remarks 3.4 and 3.6]) holds even if the family $((G_d, \rho_d, \mathcal{R}_d) \mid d \in D)$ is weakly pseudo-free in $\mathfrak{V}$ with respect to $\mathcal{D}$ and σ. The definition of weak pseudo-freeness can be obtained from the definition of pseudo-freeness by requiring the equations to be variable-free.

Also, in [1, Remark 4.4],

$$(F_{2^{\kappa(e)}}/H_{1^{\kappa(e)},e}, \rho'_{1^{\kappa(e)},e}, \mathcal{R}_{1^{\kappa(e)}} \mid e \in E)$$

should be understood as

$$((F_{2^{\kappa(e)}}/H_{1^{\kappa(e)},e}, \rho'_{1^{\kappa(e)},e}, \mathcal{R}_{1^{\kappa(e)}}) \mid e \in E).$$

References

[1] M. Anokhin, Constructing a pseudo-free family of finite computational groups under the general integer factoring intractability assumption, *Groups Complex. Cryptol.* **5** (2013), no. 1, 53–74.