Two Simple Composition Theorems with H-coefficients

Jacques Patarin

Laboratoire de Mathématiques de Versailles, UVSQ,
CNRS, Université Paris-Saclay, 78035 Versailles, France
jpatarin@club-internet.fr

Abstract. We will present here two simple theorems that show that when we compose permutation generators with independent keys, then the "quality" of CCA security increases. These theorems are written in terms of H-coefficients.

1 A simple mathematical property

Theorem 1. *Let $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ be real numbers and let α and β be real numbers, $\alpha \geq 0$, $\beta \geq 0$ such that:*
• $\sum_{i=0}^{n} x_i = 0$.
• $\sum_{i=0}^{n} y_i = 0$.
•$\forall i$, $1 \leq i \leq n$, $x_i \geq -\alpha$.
•$\forall i$, $1 \leq i \leq n$, $y_i \geq -\beta$.
Then: $\sum_{i=1}^{n} x_i y_i \geq -n\alpha\beta$.

Proof. $\forall i$, $1 \leq i \leq n$, let:

$$\begin{array}{ll} A_i = x_i & \text{if } x_i \geq 0 \\ a_i = -x_i & \text{if } x_i < 0 \\ B_i = y_i & \text{if } y_i \geq 0 \\ b_i = -y_i & \text{if } y_i < 0 \end{array}$$

Then all the values A_i, a_i, B_i, b_i, are positive, $\sum A_i = \sum a_i$, $\sum B_i = \sum b_i$, $0 \leq a_i \leq \alpha$, $0 \leq b_i \leq \beta$. Let $P = \sum_{i=1}^{n} x_i y_i$. In P, we have 4 types of terms: $A_i B_i$, $-A_i b_i$, $-a_i B_i$ and $a_i b_i$. We can assume that we have at least one term $-A_i b_i$ or $-a_i B_i$ because if this is not the case, then $P \geq 0 \geq -n\alpha\beta$. From now on, we will assume that we have at least one term $-a_{i_0} B_{i_0}$ (but not necessary one term $A_i b_i$). Without loss of generality, we can assume that we have no term in $A_i B_i$ since decreasing B_i to 0 and increasing B_{i_0} of the same value (B_{i_0} becomes $B_{i_0} + B_i$) keeps $\sum B_i = \sum b_i$ but can only decrease P (because the term in $A_i B_i$ is nonnegative and the term in $-a_{i_0} B_{i_0}$ is nonpositive), and we look for P as small as possible. Now, since we have no term in $A_i B_i$, we can assume that we have at least one term $A_{j_0} b_{j_0}$ (if not we would have no term A_i at all and since $\sum A_i = \sum a_i$, no term $a_i \neq 0$ also). Then without loosing generality, we can assume that $a_{i_0} = \alpha$ since increasing a_{i_0} and increasing A_{j_0} of the same value can only decrease P. Similarly, we can assume that all the terms

$-a_iB_i$ are $-\alpha B_i$ and all the terms $-A_ib_i$ are $-\beta A_i$.
Now, from the term in $-A_{j_0}\beta$ we see that we can assume that in all the terms a_ib_i, we have $a_i = \alpha$ since by increasing a_i to α and increasing A_{j_0} of the same value $\alpha - a_i$ (in order to keep $\sum A_i = \sum a_i$), we will only decrease P (since P is changed on $P + (\alpha - a_i)b_i - (\alpha - a_i) \leq P$). Similarly, from the term in $-\alpha B_{i_0}$, we see that we can assume that in the term a_ib_i we have $b_i = \beta$. Finally, we have found that

$$P \geq -\sum_{i=1}^{n_1} \beta A_i - \sum_{i=n_1+1}^{n_2} \alpha B_i + \sum_{i=n_2+1}^{n} \alpha\beta$$

with

$$\sum_{i=1}^{n_1} A_i = \sum a_i = ((n_2 - n_1) + (n - n_2))\, \alpha = (n - n_1)\alpha$$

$$\sum_{i=n_1+1}^{n_2} B_i = \sum b_i = (n_1 + (n - n_2))\, \beta$$

$$P \geq -(n - n_1)\alpha\beta - (n_1 + n - n_2)\alpha\beta + (n - n_2)\alpha\beta$$

Thus $P \geq -n\alpha\beta$, as claimed. □

2 A composition Theorem in CCA with H-coefficients

Theorem 2. *Let G_1 and G_2 two permutation generators (with the same key space K) such that:*
(1) For all sequences of pairwise distinct elements a_i, $1 \leq i \leq q$, and for all sequences of pairwise distinct elements b_i, $1 \leq i \leq q$, we have: $H_1 \geq \frac{|K|}{2^N(2^N-1)\ldots(2^N-q+1)}(1-\alpha_1)$ and similarly $H_2 \geq \frac{|K|}{2^N(2^N-1)\ldots(2^N-q+1)}(1-\alpha_2)$ where H_1 denotes the H coefficient for G_1 and H_2 the H coefficient for G_2. Then:
(2) If we compose 2 such generators G_1 and G_2 with random independent keys, for the composition generator $G' = G_2 \circ G_1$, we have: for all sequences of pairwise distinct elements a_i, $1 \leq i \leq q$, and for all sequences of pairwise distinct elements b_i, $1 \leq i \leq q$, $H' \geq \frac{|K|^2}{2^N(2^N-1)\ldots(2^N-q+1)}(1-\alpha_1\alpha_2)$, where H' denotes the H coefficient for G'.

Proof. Let $\tilde{H}_1$ (respectively $\tilde{H}_2$) denotes the mean value of H_1. (respectively H_2). We have:

$$\tilde{H}_1 = \tilde{H}_2 = \frac{|K|}{2^N(2^N-1)\ldots(2^N-q+1)}$$

Let denote by $\tilde{H}'$ the mean value of H for $G' = G_2 \circ G_1$. We have

$$\tilde{H}' = \frac{|K|^2}{2^N(2^N-1)\ldots(2^N-q+1)}$$

Let $a = (a_1, \dots, a_q)$ be q pairwise distinct plaintexts, and $b = (b_1, \dots, b_q)$ be q ciphertexts of G'. Let J be the set of all $(t_1, \dots, t_q)$ pairwise distinct values of $\{0,1\}^N$. We have $|J| = 2^N(2^N-1)\dots(2^N-q+1)$. For $G' = G_2 \circ G_1$, we have:

$$H(a,b) = \sum_{t \in J} H_1(a,t) H_2(t,b)$$

We also have $\sum_{t\in J} H_1(a,t) = |K|$ and $\sum_{t\in J} H_2(t,b) = |K|$ since each key sends a value a to a specific value t. We also have $|K| = \tilde{H}_1 \cdot |J| = \tilde{H}_2 \cdot |J|$. By hypothesis, we also have:

$$\forall t \in J,\, H_1(a,t) \geq \tilde{H}_1(1-\alpha_1) \ \text{ and } H_2(a,t) \geq \tilde{H}_2(1-\alpha_2)$$

$\forall t \in J$, let $x_t = \frac{H_1(a,t)}{\tilde{H}_1} - 1$ and $y_t = \frac{H_2(a,t)}{\tilde{H}_2} - 1$. $\forall t \in J$, we have $x_t \geq -\alpha_1$, and $y_t \geq -\alpha_2$, $\sum_{t\in J} x_t = 0$ and $\sum_{t \in J} y_t = 0$. Therefore, from theorem 1, we have $\sum_{t\in J} x_t y_t \geq -|J|\alpha_1\alpha_2$. For $G' = G_2 \circ G_1$, we have:

$$\begin{aligned} H(a,b) &= \textstyle\sum_{t\in J} H_1(a,t) \cdot H_2(t,b) \\ &= \textstyle\sum_{t\in J} \left(\tilde{H}_1 x_t - \tilde{H}_1\right)\left(\tilde{H}_2 y_t - \tilde{H}_2\right) \\ &= \textstyle\sum_{t\in J} \tilde{H}_1\tilde{H}_2 x_t y_t - \tilde{H}_1\tilde{H}_2 y_t - \tilde{H}_1\tilde{H}_2 x_t + \tilde{H}_1\tilde{H}_2 \\ &\geq -\tilde{H}_1\tilde{H}_2|J|\alpha_1\alpha_2 + |J|\tilde{H}_1\tilde{H}_2 \end{aligned}$$

Moreover $\tilde{H}' = \frac{|K|^2}{|J|} = |J|\tilde{H}_1\tilde{H}_2$. We have proved: $H(a,b) \geq \tilde{H}'(1-\alpha_1\alpha_2)$ as claimed. □

Theorem 3. *(H-coefficient technique, sufficient condition for security against CCA)*

Let α and β be real numbers, $\alpha > 0$ and $\beta > 0$

If: There exists a subset E of $(\{0,1\}^{qN})^2$ such that

(1a) For all $(a,b) \in E$, we have:

$$H \geq \frac{|K|}{2^{Nq}}(1-\alpha)\,\overset{\circ}{1}$$

with

$$\overset{\circ}{1} \overset{d\acute{e}f}{=} \frac{1}{(1-\frac{1}{2^N})(1-\frac{2}{2^N})\dots(1-\frac{q-1}{2^N})}$$

(1b) For all CCA acting on a random permutation f of $\mathcal{P}_N$, the probability that $(a,b) \in E$ is $\geq 1-\beta$ where (a,b) denotes here the successive $b_i = f(a_i)$ or $a_i = f^{-1}(b_i)$, $1 \leq i \leq q$, that will appear.

Then

(2) For every CCA with q queries (i.e. q chosen plaintexts or ciphertexts) we have: $\mathbf{Adv}^{PRP} \leq \alpha + \beta$ where $\mathbf{Adv}^{PRP}$ denotes the probability to distinguish $G(f_1, \dots, f_r)$ when $(f_1, \dots, f_r) \in_R K$ from a permutation $f \in_R \mathcal{P}_N$.

Proof. This theorem is proved in [5, 6]. □

Corollary 1. *From theorem 3 (H-coefficients in CCA) with* $\beta = 0$*, we see that we have:* $\mathbf{Adv}^{PRP} \leq \alpha_1\alpha_2$ *where* $\mathbf{Adv}^{PRP}$ *denotes the advantage in CCA to distinguish* $G_2 \circ G_1$ *(when the keys are independently and randomly chosen) from a permutation* $f \in_R \mathcal{P}_n$*.*

By induction, we see:

Theorem 4. *Let* q *and* k *be two integers. Let* $\alpha_1, \ldots, \alpha_k$ *be* k *real values. Let* $G_1, \ldots, G_k$ *be* k *permutation generators such that: for all sequences of pairwise distinct elements* a_i*, and for all sequences of pairwise distinct elements* b_i*,* $1 \leq i \leq q$*, we have:*

$$H \geq \frac{|K|}{2^N(2^N-1)\ldots(2^N-q+1)}(1-\alpha_j)$$

If we compose k *such generators* $G_1, \ldots, G_k$ *with random and independent keys, for the composition generator* $G' = G_k \circ \ldots \circ G_1$*, we have: for all sequences of pairwise distinct elements* a_i*,* $1 \leq i \leq q$ *and for all sequences of pairwise distinct elements* b_i*,* $1 \leq i \leq q$*,* $H \geq \frac{|K|}{2^N(2^N-1)\ldots(2^N-q+1)}(1-\alpha_1\ldots\alpha_k)$*. Therefore, from theorem 3 with* $\beta = 0$*, we see that we have:* $\mathbf{Adv}^{PRP} \leq \alpha_1 \ldots \alpha_k$

3 A composition theorem to eliminate a "hole"

J denotes, as above, the set of all q pairwise distinct values of $\{0,1\}^N$.

Theorem 5. *Let* G_1 *and* G_2 *be two permutation generators with the same key space* K*. Let* H_1 *(respectively* H_2*) denotes the H-coefficients for* G_1 *(respectively* G_2*).*

If:

(1) For all sequences of pairwise distinct elements a_i*,* $1 \leq i \leq q$*, and for all sequences of pairwise distinct* $b_i \in E_1$*,* $1 \leq i \leq q$*, we have*

$$H_1 \geq \frac{|K|}{2^N(2^N-1)\ldots(2^N-q+1)}(1-\alpha_1)$$

with $|E_1| \geq |J|(1-\epsilon_1)$*.*

(2) Similarly, for all sequences of pairwise distinct elements a_i*,* $1 \leq i \leq q$*, and for all sequences of pairwise distinct* $b_i \in E_2$*,* $1 \leq i \leq q$*, we have*

$$H_2 \geq \frac{|K|}{2^N(2^N-1)\ldots(2^N-q+1)}(1-\alpha_2)$$

with $|E_2| \geq |J|(1-\epsilon_2)$*.*

Then: for the composition generator $G_2^{-1} \circ G_1$*, for all sequences of pairwise distinct elements* a_i*, and for all sequences of pairwise distinct* b_i*, we have*

$$H' \geq \frac{|K|^2}{2^N(2^N-1)\ldots(2^N-q+1)}(1-\epsilon_1-\epsilon_2)(1-\alpha_1)(1-\alpha_2)$$

where H' denotes the H-coefficients for $G_2^{-1} \circ G_1$ (wa have no hole). Moreover, if $E_1 = E_2$, then

$$H' \geq \frac{|K|^2}{2^N(2^N-1)\dots(2^N-q+1)}(1-\epsilon_1)(1-\alpha_1)(1-\alpha_2)$$

Proof. For $G' = G_2^{-1} \circ G_1$, we have: $H'(a,b) = \sum_{t\in J} H_1(a,t)H_2(t,b)$, with $\sum_{t\in J} H_1(a,t) = |K|$ and $\sum_{t\in J} H_2(t,b) = |K|$. Let $\tilde{H}_1 = \frac{|K|}{|J|}$, $\tilde{H}_2 = \frac{|K|}{|J|}$, and $\tilde{H}' = \frac{|K|^2}{|J|} = \tilde{H}_1\tilde{H}_2|J|$. We have: $|J| = 2^N(2^N-1)\dots(2^N-q+1)$. Let $P_1 = J \setminus E_1$ and $P_2 = J \setminus E_2$. Then

$$\begin{aligned}
H'(a,b) &\geq \sum_{t\in J\setminus P_1\setminus P_2} H_1(a,t)H_2(t,b)\\
&\geq \sum_{t\in J\setminus P_1\setminus P_2} \tilde{H}_1(1-\alpha_1)\tilde{H}_2(1-\alpha_2)\\
&\geq |J\setminus P_1\setminus P_2|\tilde{H}_1(1-\alpha_1)\tilde{H}_2(1-\alpha_2)\\
&\geq |J|(1-\epsilon_1-\epsilon_2)\tilde{H}_1(1-\alpha_1)\tilde{H}_2(1-\alpha_2)\\
&\geq \frac{|K|^2}{|J|}(1-\epsilon_1-\epsilon_2)(1-\alpha_1)(1-\alpha_2)
\end{aligned}$$

as claimed. □

4 Comments about the composition theorems

These very simple theorems of composition are not very well known because the classical theorems of composition (with more difficult proofs) usually do not consider hypothesis in term of the values on the H coefficients. For example, the famous "two weak make one strong" theorem of Maurer and Pietrzak [2, 3] says that if F and G are NCPA secure, then the composition $G^{-1} \circ F$ is CCA secure. This result only holds in the information-theoretic setting, not in the computational setting (cf [4, 7]). Another example is this theorem [1]:

Theorem 6. *Let E, F and G be 3 block ciphers with the same message space M. Denote $\epsilon_E = \mathbf{Adv}_E^{NCPA}(q)$, $\epsilon_F = \mathbf{Adv}_F^{NCPA}(q)$, $\epsilon_{F^{-1}} = \mathbf{Adv}_{F^{-1}}^{NCPA}(q)$ and $\epsilon_{G^{-1}} = \mathbf{Adv}_{G^{-1}}^{NCPA}(q)$, where q is the number of queries. We have:*

$$\mathbf{Adv}_{G\circ F\circ E}^{CCA}(q) \leq \epsilon_E\epsilon_F + \epsilon_E\epsilon_{G^{-1}} + \epsilon_{F^{-1}}\epsilon_{G^{-1}} + \min\left\{\epsilon_E\epsilon_F, \epsilon_E\epsilon_{G^{-1}}, \epsilon_{F^{-1}}\epsilon_{G^{-1}}\right\}$$

Why do we have 3 rounds in this theorem and only 2 rounds in theorem 2 for the product of the advantages? (Moreover theorem 6 was also proved by using the H-coefficient technique [1]). This is because in theorem 2, we used the additional property that there are no "holes" in the hypothesis that H is greater than or equal to the mean value $H(1-\epsilon)$, i.e. that this property was true for any q pairwise distinct inputs and q pairwise distinct outputs.

References

1. Cogliati, B., Patarin, J., Seurin, Y.: Security Amplification for the Composition of Block Cipher: Simpler Proofs and New Results. Selected Areas in Cryptography–SAC '14, A. Joux, A. Yousssef (eds), 129-146, Springer-Verlag, Lecture Notes in Computer Science, 8781, (2014)
2. Maurer, U.: Indistinguishability of Random Systemes. Advances in Cryptology – EUROCRYPT '02, L.R. Knudsen (ed), 110-132, Springer-Verlag, Lecture Notes in Computer Science, 2332, (2002)
3. Maurer, U., Pietrzak, K., Renner, R.: Indistinguishability Amplification. Advances in Cryptology – CRYPTO '07, A. Menezes (ed), 130-149, Springer-Verlag, Lecture Notes in Computer Science, 4622, (2007)
4. Myers, S.: Black-Box Composition Does Not Imply Adaptive Security. Advances in Cryptology – EUROCRYPT '04, C. Cachin, J.L. Camenisch (eds), 189-206, Springer-Verlag, Lecture Notes in Computer Science, 3027, (2004)
5. J. Patarin, *Étude des Générateurs de Permutations Pseudo-aléatoires basés sur le schéma du D.E.S.*, PhD, November 1991.
6. Patarin, J.: The "coefficient H" technique. Selected Areas in Cryptography – SAC '08, R. Avanzi, L. Keliher, F. Sica (eds), 328-345, Springer-Verlag, Lecture Notes in Computer Science, 5381, (2009)
7. Pietrzak, K.: Composition Does Not Imply Adaptive Security.. Advances in Cryptology – CRYPTO '05, V. Shoup (ed), 55-65, Springer-Verlag, Lecture Notes in Computer Science, 3621, (2005)