Security Amplification for the Composition of Block Ciphers: Simpler Proofs and New Results

B. Cogliati [1] J. Patarin [1] Y. Seurin [2]

[1]University of Versailles, FRANCE

[2]ANSSI, FRANCE

November 12, 2014

We consider the general problem of *security amplification* for blockciphers:

Problem

Given two or more blockciphers $E, F \ldots$ does the composition $E \circ F \cdots$ offer better security than each component?

- widely studied problem, lots of results in different models (computational model, information-theoretic model, ideal cipher model,...)
- we focus here on the information-theoretic model (computationally unbouded adversaries)
- starting point of our work: the famous "Two weak make one strong" theorem

Theorem (2W1S theorem)

If E and F are (q, ϵ) secure against chosen plaintext non-adaptive (NCPA) adversaries, then $F^{-1} \circ E$ is $(q, 2\epsilon)$-secure against chosen plaintext and ciphertext (CCA) adversaries

Previous proof was long and complex [Mau02, MPR07, JÖS12].

Our results in short

- we give a surpringly simple proof of the 2W1S theorem,
- we extend it to any number of rounds.

The distinguishing advantage of an adversary

Fix a block cipher E with key space $\mathcal{K}$ and message space $\mathcal{M}$. A distinguisher D is an algorithm with oracle access to a permutation F which outputs a bit D^F.

His advantage is

$$\left|\Pr\left[K \leftarrow_{\$} \mathcal{K} : D^{E_K} = 1\right] - \Pr\left[P \leftarrow_{\$} \mathrm{Perm}(\mathcal{M}) : D^P = 1\right]\right|.$$

$\mathbf{Adv}_E^{\mathrm{cca}}(q)$: maximum advantage when D is limited to q queries.
$\mathbf{Adv}_E^{\mathrm{ncpa}}(q)$: maximum advantage when D is limited to q non-adaptive forward queries.
$\mathbf{Adv}_E^{\mathrm{cpa}}(q)$: maximum advantage when D is limited to q adaptive forward queries.

A preview of the results

Composing block cipher with independant keys improves security:

- the gain for ncpa and cpa security is geometric,
- to achieve the same level of cca security from ncpa-secure block ciphers, one must double the length of the cascade.

We show that only one round must be added to get roughly the same level of cca security.

A preview of the results

Composing block cipher with independant keys improves security:

- the gain for ncpa and cpa security is geometric,
- to achieve the same level of cca security from ncpa-secure block ciphers, one must double the length of the cascade.

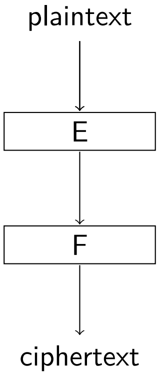
We show that only one round must be added to get roughly the same level of cca security.

Security amplification

2 types of security amplification:

- ϵ-amplification,
- class amplification.

Example of $\epsilon-$amplification (from [Vau98, Vau99])



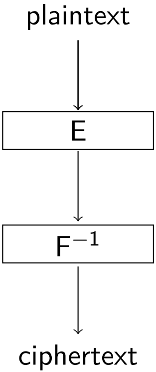
E is $(q, \epsilon_E)-$NCPA (resp. CPA) secure.

F is $(q, \epsilon_F)-$NCPA (resp. CPA) secure.

$\rightarrow$ We get a $(q, 2\epsilon_E\epsilon_F)-$NCPA (resp CPA) secure blockcipher.

Example of class amplification

"Two weak make one strong" (TW1S) theorem



E is $(q, \epsilon_E)-$NCPA secure.

F is $(q, \epsilon_F)-$NCPA secure.

$\rightarrow$ We get a $(q, \epsilon_E + \epsilon_F)-$CCA secure blockcipher.

Example of class amplification

"Two weak make one strong" (TW1S) theorem

This theorem is used in several proofs [MRS09, HR10, LPS12, LS14].

However its proof relies on three articles : [Mau02], [MPR07] and [JÖS12].

Example of class amplification

"Two weak make one strong" (TW1S) theorem

This theorem is used in several proofs [MRS09, HR10, LPS12, LS14].

However its proof relies on three articles : [Mau02], [MPR07] and [JÖS12].

Stastistical distance

Let μ and ν be 2 probability distributions on a finite event space Ω. The stastistical distance between μ and ν is:

$$\begin{aligned}\|\mu - \nu\| &= \frac{1}{2}\sum_{\omega \in \Omega} |\mu(\omega) - \nu(\omega)| \\ &= \sum_{\substack{\omega \in \Omega \\ \mu(\omega) > \nu(\omega)}} (\mu(\omega) - \nu(\omega))\end{aligned}$$

Some notations

Let x, y be $q-$tuples of pairwise distinct messages from $\mathcal{M}$ and E a block cipher with message space $\mathcal{M}$. Then

- $\mathrm{p}_E(x, y)$ is the probability, over the choice of the key, that E outputs y with input x,
- $\mathrm{p}_{E,x}$ is the probability distribution of the outputs of E when the input x is fixed,
- $\mathrm{p}^* = \frac{1}{|\mathcal{M}|(|\mathcal{M}|-1)\ldots(|\mathcal{M}|-q+1)}$.

Some notations

Let x, y be $q-$tuples of pairwise distinct messages from $\mathcal{M}$ and E a block cipher with message space $\mathcal{M}$. Then

- $\mathrm{p}_E(x, y)$ is the probability, over the choice of the key, that E outputs y with input x,
- $\mathrm{p}_{E,x}$ is the probability distribution of the outputs of E when the input x is fixed,
- $\mathrm{p}^* = \frac{1}{|\mathcal{M}|(|\mathcal{M}|-1)\ldots(|\mathcal{M}|-q+1)}$.

Some notations

Let x, y be $q-$tuples of pairwise distinct messages from $\mathcal{M}$ and E a block cipher with message space $\mathcal{M}$. Then

- $\mathrm{p}_E(x, y)$ is the probability, over the choice of the key, that E outputs y with input x,
- $\mathrm{p}_{E,x}$ is the probability distribution of the outputs of E when the input x is fixed,
- $\mathrm{p}^* = \frac{1}{|\mathcal{M}|(|\mathcal{M}|-1)\dots(|\mathcal{M}|-q+1)}$.

Fundamental results of the H-coefficient method

Lemma

Let E be a block cipher with message space $\mathcal{M}$. Denote $(\mathcal{M})_q$ the set of $q-$tuples of pairwise distinct messages of $\mathcal{M}$. Then

$$\mathbf{Adv}_E^{\mathrm{ncpa}}(q) = \max_{x \in (\mathcal{M})_q} \|\mathsf{p}_{E,x} - \mathsf{p}^*\|.$$

Fundamental results of the H-coefficient method

Lemma

Let E be a block cipher with message space $\mathcal{M}$. Assume that there exists ϵ such that for any $q-$tuples $x, y \in (\mathcal{M})_q$, one has

$$\mathrm{p}_E(x, y) \geq (1 - \epsilon)\mathrm{p}^*.$$

Then

$$\mathbf{Adv}_E^{\mathrm{cca}}(q) \leq \epsilon.$$

A proof of the 2W1S theorem

Let E and F be two block ciphers with the same message space $\mathcal{M}$ and respective key spaces $\mathcal{K}_E$ and $\mathcal{K}_F$. Let $x, y \in (\mathcal{M})_q$.

First step: a surprisingly simple and useful formula:

$$\mathrm{p}_{F^{-1}\circ E}(x,y) = \mathrm{p}^* + \sum_{z\in(\mathcal{M})_q} (\mathrm{p}_E(x,z) - \mathrm{p}^*)(\mathrm{p}_F(y,z) - \mathrm{p}^*)$$

A proof of the 2W1S theorem

Let E and F be two block ciphers with the same message space $\mathcal{M}$ and respective key spaces $\mathcal{K}_E$ and $\mathcal{K}_F$. Let $x, y \in (\mathcal{M})_q$.

First step: a surprisingly simple and useful formula:

$$\mathrm{p}_{F^{-1}\circ E}(x,y) = \mathrm{p}^* + \sum_{z \in (\mathcal{M})_q} (\mathrm{p}_E(x,z) - \mathrm{p}^*)(\mathrm{p}_F(y,z) - \mathrm{p}^*)$$

A proof of the 2W1S theorem

$$\begin{aligned} \mathrm{p}_{F^{-1}\circ E}(x,y) \geq{} & \mathrm{p}^* + \sum_{\substack{z\in(\mathcal{M})_q \\ \mathrm{p}_E(x,z)>\mathrm{p}^* \\ \mathrm{p}_F(y,z)<\mathrm{p}^*}} \underbrace{(\mathrm{p}_E(x,z)-\mathrm{p}^*)}_{>0}\underbrace{(\mathrm{p}_F(y,z)-\mathrm{p}^*)}_{\geq -\mathrm{p}^*} \\ & + \sum_{\substack{z\in(\mathcal{M})_q \\ \mathrm{p}_E(x,z)<\mathrm{p}^* \\ \mathrm{p}_F(y,z)>\mathrm{p}^*}} \underbrace{(\mathrm{p}_E(x,z)-\mathrm{p}^*)}_{\geq -\mathrm{p}^*}\underbrace{(\mathrm{p}_F(y,z)-\mathrm{p}^*)}_{>0} \end{aligned}$$

A proof of the 2W1S theorem

$$\begin{aligned}
\mathrm{p}_{F^{-1}\circ E}(x,y) \geq & \, \mathrm{p}^* - \mathrm{p}^* \underbrace{\sum_{\substack{z\in(\mathcal{M})_q \\ \mathrm{p}_E(x,z)>\mathrm{p}^*}} (\mathrm{p}_E(x,z)-\mathrm{p}^*)}_{\leq \mathbf{Adv}_E^{\mathrm{ncpa}}(q)} \\
& - \mathrm{p}^* \underbrace{\sum_{\substack{z\in(\mathcal{M})_q \\ \mathrm{p}_F(y,z)>\mathrm{p}^*}} (\mathrm{p}_F(y,z)-\mathrm{p}^*)}_{\leq \mathbf{Adv}_F^{\mathrm{ncpa}}(q)}
\end{aligned}$$

Then

$$\mathrm{p}_{F^{-1}\circ E}(x,y) \geq \mathrm{p}^*(1 - \mathbf{Adv}_E^{\mathrm{ncpa}}(q) - \mathbf{Adv}_F^{\mathrm{ncpa}}(q)).$$

Many weak make one even stronger!

Our proof scales very well to the composition of multiple block ciphers and gives:

Theorem

Let $E_1, \ldots, E_n$ be n block ciphers with the same message space $\mathcal{M}$. For any integer q, one has

$$\mathbf{Adv}^{\mathrm{cca}}_{E_n \circ \ldots \circ E_1}(q) \leq 2^{n-1} \max_{1 \leq i \leq n} \left(\prod_{j=1}^{i-1} \mathbf{Adv}^{\mathrm{ncpa}}_{E_j}(q) \times \prod_{j=i+1}^{n} \mathbf{Adv}^{\mathrm{ncpa}}_{E_j^{-1}}(q) \right).$$

Many weak make one even stronger!

Corollary

Let E be a block cipher and $q \geq 1$. Denote $\epsilon = \max\{\mathbf{Adv}_E^{\mathrm{ncpa}}(q), \mathbf{Adv}_{E^{-1}}^{\mathrm{ncpa}}(q)\}$. Then, for any integer $n \geq 1$,

$$\mathbf{Adv}_{E^n}^{\mathrm{cca}}(q) \leq (2\epsilon)^{n-1}.$$

The best we could get using previous results was:

- $\mathbf{Adv}_{E^n}^{\mathrm{cca}}(q) \leq (2\epsilon)^{n/2}$ when n is even,
- $\mathbf{Adv}_{E^n}^{\mathrm{cca}}(q) \leq (2\epsilon)^{\frac{n-1}{2}} \frac{1+2\epsilon}{2}$ when n is odd.

About the tightness of MW1S

Denote G the block cipher whose key space is the set of all permutations of $\mathcal{M}$ such that 0 lies in a circle of length 2 and F the block cipher such that:

- with probability ϵ, F is the identity function $\mathcal{I}$,
- with probability $1-\epsilon$, F is G with a uniformly random key.

Then

$$\mathbf{Adv}_{F^n}^{\mathrm{cca}}(q) \gtrapprox n \cdot \mathbf{Adv}_{F}^{\mathrm{ncpa}}(q)^{n-1}$$

when $\mathcal{M}$ is sufficiently large and ϵ sufficiently small.

Composition of 3 block ciphers

Theorem

Let E, F, G be 3 block ciphers with the same message space $\mathcal{M}$ and q be any positive integer. Denote, for any block cipher B, $\epsilon_B := \mathbf{Adv}_B^{\mathrm{ncpa}}(q)$. Then

$$\begin{aligned}\mathbf{Adv}_{G\circ F\circ E}^{\mathrm{cca}}(q) \leq & \epsilon_E\epsilon_F + \epsilon_E\epsilon_{G^{-1}} + \epsilon_{F^{-1}}\epsilon_{G^{-1}} \\ & + \min\{\epsilon_E\epsilon_F, \epsilon_E\epsilon_{G^{-1}}, \epsilon_{F^{-1}}\epsilon_{G^{-1}}\}.\end{aligned}$$

In summary,

- we give a new simple proof of the "Two weak make one strong" theorem, relying on the H-coefficients framework [Pat08],
- we extend the 2W1S theorem to any number of rounds, and show that if E and E^{-1} are (q, ϵ)-ncpa secure, then E^n is $(q, (2\epsilon)^{n-1})$-secure,
- in particular, this shows that 3 rounds are sufficient to provide *both* $\epsilon-$amplification and class amplification (E and E^{-1} (q, ϵ)-ncpa secure $=>$ E^3 is $(q, 4\epsilon^2)$-cca secure),
- our extension is tight up to some constant factor.

In summary,

- we give a new simple proof of the "Two weak make one strong" theorem, relying on the H-coefficients framework [Pat08],
- we extend the 2W1S theorem to any number of rounds, and show that if E and E^{-1} are (q,ϵ)-ncpa secure, then E^n is $(q,(2\epsilon)^{n-1})$-secure,
- in particular, this shows that 3 rounds are sufficient to provide *both* $\epsilon-$amplification and class amplification (E and E^{-1} (q,ϵ)-ncpa secure $=>$ E^3 is $(q,4\epsilon^2)$-cca secure),
- our extension is tight up to some constant factor.

In summary,

- we give a new simple proof of the "Two weak make one strong" theorem, relying on the H-coefficients framework [Pat08],
- we extend the 2W1S theorem to any number of rounds, and show that if E and E^{-1} are (q, ϵ)-ncpa secure, then E^n is $(q, (2\epsilon)^{n-1})$-secure,
- in particular, this shows that 3 rounds are sufficient to provide *both* $\epsilon-$amplification and class amplification (E and E^{-1} (q, ϵ)-ncpa secure $=>$ E^3 is $(q, 4\epsilon^2)$-cca secure),
- our extension is tight up to some constant factor.

In summary,

- we give a new simple proof of the "Two weak make one strong" theorem, relying on the H-coefficients framework [Pat08],
- we extend the 2W1S theorem to any number of rounds, and show that if E and E^{-1} are (q, ϵ)-ncpa secure, then E^n is $(q, (2\epsilon)^{n-1})$-secure,
- in particular, this shows that 3 rounds are sufficient to provide *both* $\epsilon-$amplification and class amplification (E and E^{-1} (q, ϵ)-ncpa secure $=>$ E^3 is $(q, 4\epsilon^2)$-cca secure),
- our extension is tight up to some constant factor.

Thank you!

Viet Tung Hoang and Phillip Rogaway.
On Generalized Feistel Networks.
In Tal Rabin, editor, *Advances in Cryptology - CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 613–630. Springer, 2010.

Dimitar Jetchev, Onur Özen, and Martijn Stam.
Understanding Adaptivity: Random Systems Revisited.
In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 313–330. Springer, 2012.

Rodolphe Lampe, Jacques Patarin, and Yannick Seurin.
An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher.
In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 278–295. Springer, 2012.

Rodolphe Lampe and Yannick Seurin.
Security Analysis of Key-Alternating Feistel Ciphers.
In *Fast Software Encryption - FSE 2014*, 2014.
To appear.

Ueli M. Maurer.
Indistinguishability of Random Systems.
In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 110–132. Springer, 2002.

Ueli M. Maurer, Krzysztof Pietrzak, and Renato Renner.
Indistinguishability Amplification.
In Alfred Menezes, editor, *Advances in Cryptology - CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 130–149. Springer, 2007.
Full version available at `http://eprint.iacr.org/2006/456`.

Ben Morris, Phillip Rogaway, and Till Stegers.
How to Encipher Messages on a Small Domain.
In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 286–302. Springer, 2009.

Jacques Patarin.
The "Coefficients H" Technique.
In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography - SAC 2008*, volume 5381 of *Lecture Notes in Computer Science*, pages 328–345. Springer, 2008.

Serge Vaudenay.
Provable Security for Block Ciphers by Decorrelation.
In Michel Morvan, Christoph Meinel, and Daniel Krob, editors, *Symposium on Theoretical Aspects of Computer Science, STACS 98*, volume 1373 of *Lecture Notes in Computer Science*, pages 249–275. Springer, 1998.

Serge Vaudenay.

Adaptive-Attack Norm for Decorrelation and Super-Pseudorandomness.

In Howard M. Heys and Carlisle M. Adams, editors, *Selected Areas in Cryptography - SAC '99*, volume 1758 of *Lecture Notes in Computer Science*, pages 49–61. Springer, 1999.