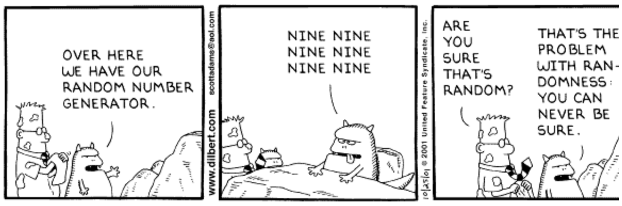
An Information-theoretic Approach to Hardness Amplification

Ueli Maurer

ETH Zurich

ISIT 2017, Aachen.

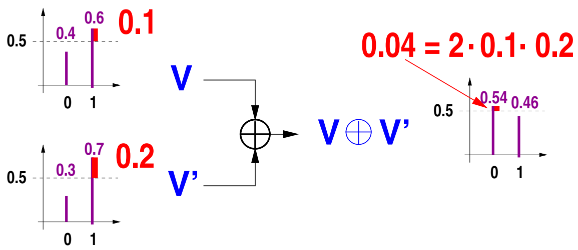
Security amplification paradigm



Idea: Combine several mildly secure systems to obtain a highly secure system.

Example: XOR of mildly uniform independent keys yields a highly uniform key!

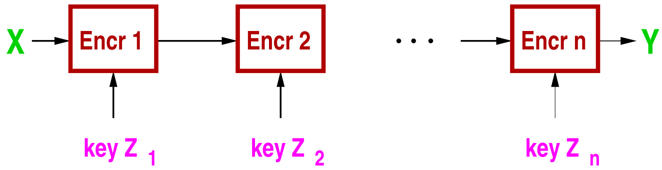
Product theorem for random variables



Product Theorem:

$$\mathbf{d}(\mathbf{V}\oplus\mathbf{V'},\mathbf{U}) \leq 2 \cdot \mathbf{d}(\mathbf{V},\mathbf{U}) \cdot \mathbf{d}(\mathbf{V'},\mathbf{U})$$

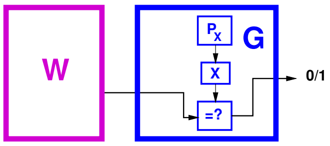
Cascade encryption



Product Theorem (informal) [M-Tessaro09]:

$$\text{Security}(\textbf{Encr 1}\cdots\textbf{Encr 1}) \approx \prod_{i=1}^{n} \text{Security}(\textbf{Encr i})$$

Winning a game G

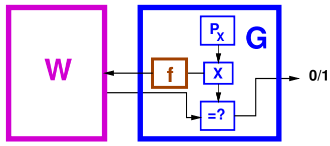


$\overline{\mathbf{G}}(\mathbf{W}) =$ probability that **W** wins game **G**

$\overline{\mathbf{G}}(\bullet) =$ maximal winning probability (best **W**)

$\overline{\mathbf{G}}(\bullet) = \max_x P_X(x)$

Winning a game G



$\overline{\mathbf{G}}(\mathbf{W}) =$ probability that **W** wins game **G**

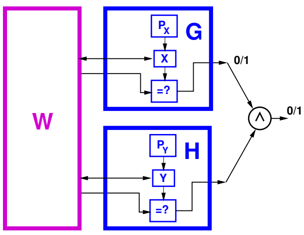
$\overline{\mathbf{G}}(\bullet) =$ maximal winning probability (best **W**)

Problem: $\overline{\mathbf{G}}(\bullet) = 1$

Computational security: $\overline{\mathbf{G}}(\mathcal{E}) \approx \beta$

f is called a β**-weak** one-way function

Winning two games G and H

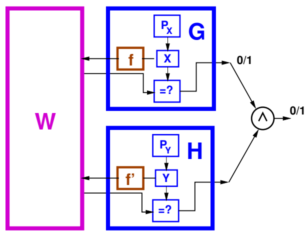


$\overline{[\mathbf{G},\mathbf{H}]^{\wedge}}(\mathbf{W}) =$ prob. that **W** wins games **G** and **H**

Product Theorem [MPR07]:

$$\overline{[\mathbf{G},\mathbf{H}]^{\wedge}}(\bullet) = \overline{\mathbf{G}}(\bullet) \cdot \overline{\mathbf{H}}(\bullet)$$

Winning two games G and H



$\overline{[\mathbf{G},\mathbf{H}]^{\wedge}}(\mathbf{W}) =$ prob. that **W** wins games **G** and **H**

Product Theorem [Goldreich,MT09]:

$$\overline{[\mathbf{G},\mathbf{H}]^{\wedge}}(\mathcal{E}) \approx \overline{\mathbf{G}}(\mathcal{E}) \cdot \overline{\mathbf{H}}(\mathcal{E})$$

Hardness and security in cryptography

Cryptographic security statement:

problem P is hard $\Rightarrow$ scheme X is secure

Definition of hard and secure?

Definition: Problem P is **hard [above β]** if no polynomial-time algorithm has success probability non-negligibly greater than β.

negligible: vanishing faster than inverse of any polynomial.

Proof methodology: A **reduction** converts any polynomial-time algorithm that breaks scheme X into a polynomial-time algorithm algorithm that solves problem P.

An apparent dilemma in computer science

"Theorem" means theorem !!!

$\Rightarrow$ One must precisely define computation, hardness, efficiency, infeasibility, non-negligible, security, ...

$\Rightarrow$ Turing machines, communication tapes, asymptotics, polynomial-time, ...

$\Rightarrow$ **enormous complexity, imprecise papers, ...**

An apparent dilemma in computer science

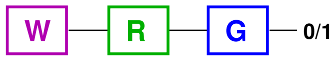
Proposed approach [M-Renner11]:

Top-down abstraction
instead of
bottom-up definitions

Goals of abstraction:

- eliminate irrelevant details, minimality
- simpler definitions
- generality of results
- simpler proofs, elegance
- didactic suitability, better understanding

Abstract games



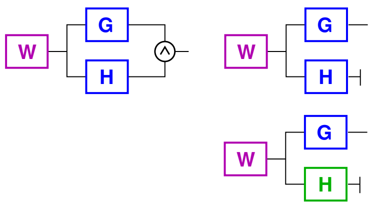
$\overline{\mathbf{G}}(\mathbf{W}) =$ probability that **W** wins game **G**

$\overline{\mathbf{RG}}(\mathbf{W}) = \overline{\mathbf{G}}(\mathbf{WR})$

Information-theoretic:

- no assumed computational model
- abstract treatment

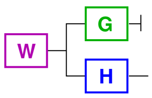
Hardness amplification for two games



= **H**

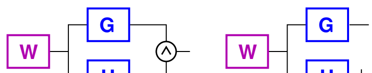
$\overline{[\mathbf{G},\mathbf{H}]^{\wedge}}(\mathbf{W}) \leq \overline{\mathbf{HG}}(\mathbf{W}) = \overline{\mathbf{G}}(\mathbf{WH})$

$\overline{[\mathbf{G},\mathbf{H}]^{\wedge}}(\mathbf{W}) \leq \overline{\mathbf{GH}}(\mathbf{W}) = \overline{\mathbf{H}}(\mathbf{WG})$



= **G**

Hardness amplification for two games



Q: Can we do better? Amplification?

We wish to show:

$\overline{[\mathbf{G},\mathbf{H}]^{\wedge}}(\mathbf{W}) \leq \overline{\mathbf{G}}(\mathbf{W'}) \cdot \overline{\mathbf{H}}(\mathbf{W''})$

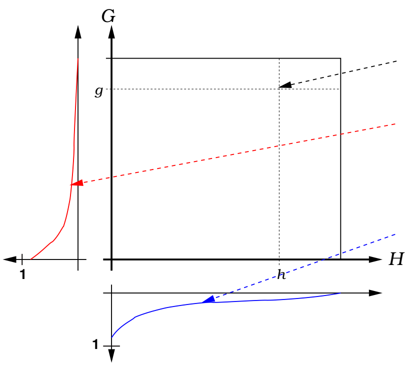
for some **W'** and **W"** derived from **W**.

Any winner **W** with $\overline{[\mathbf{G},\mathbf{H}]^{\wedge}}(\mathbf{W}) \geq 0.01$ can be used to obtain **W'** and **W"** such that either $\overline{\mathbf{G}}(\mathbf{W'}) \geq 0.1$ or $\overline{\mathbf{H}}(\mathbf{W''}) \geq 0.1$.

Success probability function of a winner W

$G =$ set of instances for the game **G**.

$H =$ set of instances for the game **H**.



$\overline{[\mathbf{g},\mathbf{h}]^{\wedge}}(\mathbf{W})$

$\mathrm{E}_{\mathbf{H}}\left[\overline{[\mathbf{g},\mathbf{H}]^{\wedge}}(\mathbf{W})\right]$

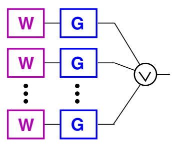
$\leq \overline{\mathbf{g}}(\mathbf{WH})$

$\mathrm{E}_{\mathbf{G}}\left[\overline{[\mathbf{G},\mathbf{h}]^{\wedge}}(\mathbf{W})\right]$

$\leq \overline{\mathbf{h}}(\mathbf{WG})$

Amplification by repetition

Idea: Repeat a given winner **W** for game **G** q times to amplify the success probability:



$\mathbf{G}^{[q]}$: q clones of **G** (same instance)

$\mathbf{W}^{q}$: q independent copies of **W**

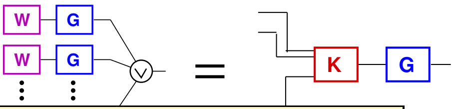
Goal: $\overline{\mathbf{G}^{[q]\vee}}(\mathbf{W}^q) > \overline{\mathbf{G}}(\mathbf{W})$

Hope: $\overline{\mathbf{G}^{[q]\vee}}(\mathbf{W}^q) = \psi_q(\overline{\mathbf{G}}(\mathbf{W}))$ for $\psi_q(x) := 1-(1-x)^q$

Problem: Game **G** must be clonable.

Amplification by repetition

Idea: Repeat a given winner **W** for game **G** q times to amplify the success probability:



$\overline{\mathsf{g}}(\mathsf{W}) \geq e \;\Rightarrow\; \overline{\mathsf{g}^{[q]^\vee}}(\mathsf{W}^q) \geq \psi_q(e) \approx 1$

$\mathsf{G}^{[q]}$: ... (same instance)

W^q : q independent copies of W

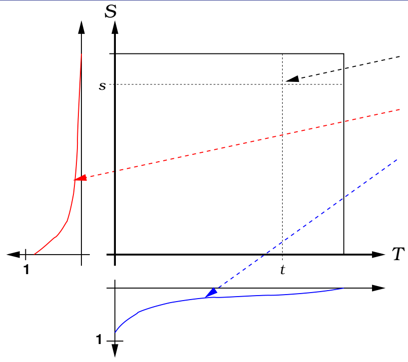
Goal: $\overline{\mathsf{G}^{[q]^\vee}}(\mathsf{W}^q) \;\geq\approx\; \Pr^{\mathsf{G}\to\mathsf{g}}\left(\overline{\mathsf{g}}(\mathsf{W}) \geq e\right)$

Hope: ... $= \psi_q(\overline{\mathsf{G}}(\mathsf{W}))$ for $\psi_q(x) := 1-(1-x)^q$

Problem: Generally false, $\overline{\mathsf{G}^{[q]^\vee}}(\mathsf{W}^q) = \overline{\mathsf{G}}(\mathsf{W})$ possible.

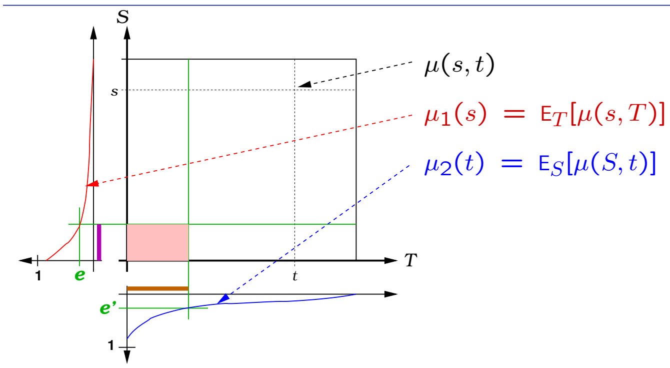
But: Holds for fixed instance **g**: $\overline{\mathsf{g}^{[q]^\vee}}(\mathsf{W}^q) = \psi_q(\overline{\mathsf{g}}(\mathsf{W}))$

A lemma on multi-argument conditional PD's



Consider a function $\mu : \mathcal{S}\times\mathcal{T} \to [0,1]$, as well as probability distributions P_S on $\mathcal{S}$ and P_T on $\mathcal{T}$, defining (independent) random variables S and T, respectively.

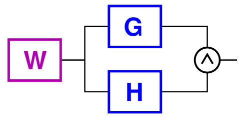
A lemma on multi-argument conditional PD's



Lemma: For every $0 \leq e, e' < 1$ and every function $\mu : \mathcal{S}\times\mathcal{T} \to [0,1]$, we have

$\mathsf{E}_{ST}[\mu(S,T)] \leq \Pr^S\left(\mu_1(S) \geq e\right) \cdot \Pr^T\left(\mu_2(T) \geq e'\right) + e + e'$

Hardness amplification for two games



Theorem: If **G** and **H** are clonable by **K** and **L**, respectively, then for any **W**, we have

$$\overline{[\mathsf{G},\mathsf{H}]^\wedge}(\mathsf{W}) \;\leq\; (1+\delta)\,\overline{\mathsf{G}}(\mathsf{W'})\cdot\overline{\mathsf{H}}(\mathsf{W''}) \;+\; \delta',$$

where $\mathsf{W'} = (\mathsf{W}\overline{\mathsf{H}})^q\mathsf{K}$ and $\mathsf{W''} = (\mathsf{W}\overline{\mathsf{G}})^q\mathsf{L}$,

for any $\delta, \delta' > 0$ and q defined by $q \;\approx\; \dfrac{2\ln(2/\delta)}{\delta'}$,

Hardness amplification for two games

Corollary: $\mathit{hard}(\mathsf{G},\beta) \;\wedge\; \mathit{hard}(\mathsf{H},\gamma) \;\Rightarrow\; \mathit{hard}([\mathsf{G},\mathsf{H}]^\wedge, \beta\gamma)$.

Corollary [Gol01]: weak OWFs exist $\Rightarrow$ strong OWFs exist.

then for any **W**, we have

$$\overline{[\mathsf{G},\mathsf{H}]^\wedge}(\mathsf{W}) \;\leq\; (1+\delta)\,\overline{\mathsf{G}}(\mathsf{W'})\cdot\overline{\mathsf{H}}(\mathsf{W''}) \;+\; \delta',$$

where $\mathsf{W'} = (\mathsf{W}\overline{\mathsf{H}})^q\mathsf{K}$ and $\mathsf{W''} = (\mathsf{W}\overline{\mathsf{G}})^q\mathsf{L}$,

for any $\delta, \delta' > 0$ and q defined by $q \;\approx\; \dfrac{2\ln(2/\delta)}{\delta'}$,