Time-Advantage Ratios under Simple Transformations: Applications to Leakage Resilient Cryptography

Maciej Skórski
University of Warsaw

BALKANCRYPT 2015
3-4 September 2015, Koper

1. Security of crypto primitives
   - Security definitions
   - Security games
   - Time/Advantage Ratio
2. Problem
   - Security loss under reductions
3. Our contribution: security loss formula
4. Applications
   - Pseudoentropy chain rules
   - Leakage-resilient stream ciphers
   - Weak pseudo-random functions
5. Conclusions

Plan

How to define security of crypto objects?

Let P be a cryptographic application, for example

- protocol
- cipher
- hash function
- pseudorandom function
- ...

We want to know how much secure is P.

Quantify the security of P

To this end, we focus on two factors

Focus on resources and success probability

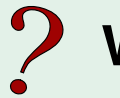
Security of crypto objects

Definition (Security)

We say that P is (t, ϵ)-secure if no adversary A with resources t can break P with advantage better than ϵ.

What are resources?

- $t =$ running time/circuit size
- $t =$ number of queries
- ...



What is advantage?

$\epsilon =$ the gain in probability of winning the security game

Example: distinguishing games

Distinguishing

Consider two distributions X_0, X_1, and the following experiment.

Step (a) Sample $b \leftarrow \{0,1\}$.

Step (b) Give X_b to A

Step (c) Ask A to guess b

One can show that the probability of guessing b by A equals

$$\Pr[A(X_b) = b] = \underbrace{\frac{1}{2}}_{\text{trivial guess}} + \underbrace{\frac{1}{2}\left(\Pr[A(X_1) = 1] - \Pr[A(X_0) = 1]\right)}_{\text{advantage } \epsilon}$$

$$\leqslant \frac{1}{2} + d_{TV}\left(X_1; X_0\right)$$

where d_{TV} is the total variation distance.

Advantage $=$ the gain over the trivial attack

The advantage of an attacker is not the winning probability, but rather the gain over the trivial attack.

Example: One-Time Pad encryption

Example (OTP with strong and weak keys)

Setting

- message $m \in \{0,1\}^{128}$
- secret key $r \leftarrow \{0,1\}^{128}$
- ciphertext $c = m \oplus r$.

Security game

- sample $b \leftarrow \{0,1\}$
- if $b = 0$ then A gets a fresh random value $r' \in \{0,1\}^{128}$
- if $b = 1$ then A gets the ciphertext $c = m \oplus r$
- A is asked to guess b (trivial strategy wins with probability $\frac{1}{2}$).

Time/Advantages pairs

Setting	Resources	Trivial guess	Guessing pr.	Advantage
uniform r	$t = 2^{128}$	$\frac{1}{2}$	$\frac{1}{2}$	$\epsilon = 0$
2 bits of r known	$t = 3$	$\frac{1}{2}$	$\frac{1}{2} + \frac{1}{2} \cdot \left(1 - \frac{1}{2^2}\right)$	$\epsilon = \frac{3}{8}$

Time-Advantage Ratio

Note that the adversary may trade time for success probability. For this reason, we need a clear and unified security measure.

Definition (Time-Success Ratio)

P has k bits of security (is 2^k-secure) if is (t, ϵ)-secure for any (t, ϵ) such that $\frac{t}{\epsilon} > 2^k$.

An easy example is the case when the brute-force search over the secret key space is the best possible attack.

Example

AES256 is believed to be (t, ϵ)-secure with any (t, ϵ) such that $\frac{t}{\epsilon} \approx 2^{256}$.

Plan

Reduction-based security proofs

Suppose that the security of P reduces to the security of P'.

Reduction

P *broken in time* t *with prob.* $\epsilon \Longrightarrow P'$ *broken in time* t' *with prob.* ϵ'

The natural question is how the security of P and P' are related?

What is the security loss?

Suppose that P' kas k' bits of security. How much secure is P?

Plan

A generic formula on the security loss

Theorem (Time-Success Ratio under Simple Reductions)

Suppose that the following holds: if P can be broken with running time t and success probability ϵ then P' can be broken with running time t' and success probability ϵ' where

$$\begin{aligned} t' &= c_1 t^{\alpha_1} \epsilon^{-\beta_1} + c_3 \epsilon^{-\beta_3} \\ \epsilon' &= c_2 t^{-\alpha_2} \epsilon^{\beta_2}. \end{aligned} \tag{1}$$

and $\alpha_1, \alpha_2, c_1, c_2, c_3, \beta_1, \beta_2, \beta_3$ are positive constants. Then the following holds: if P' is K'-secure then P is K-secure where K' and K satisfy

$$K' = (1+\psi) \cdot \max\left(\frac{c_1}{c_2} \cdot K^{\max(\alpha_1+\alpha_2, \beta_1+\beta_2)}, \frac{c_3}{c_2} \cdot K^{\max(\alpha_2, \beta_2+\beta_3)} \right) \tag{2}$$

for some parameter $0 \leqslant \psi \leqslant 1$.

Plan

Pseudoentropy chain rules comparison

Reference	Technique	$t' =$	$\epsilon' =$	Security Loss **our contribution**
(a) [DP08]	Worst-Case Metric Entropy	$O\left(t \cdot 2^{-2\lambda}\epsilon^{-2}\right)$	$\Omega(2^{-\lambda}\epsilon^2)$	$k \approx \frac{k'}{4} - \frac{3}{4}\lambda$
(b) [RTTV08]	Dense Model Theorem	$O\left(t \cdot \mathrm{poly}(\frac{1}{\epsilon}, \frac{1}{\min_z(\Pr[Z=z])})\right)$	$\Omega(2^{-\lambda}\epsilon)$	worse than in (c)
(c) [FOR15]	Worst-Case Metric Entropy	$O\left(t \cdot 2^{-2\lambda}\epsilon^{-2}\right)$	$\Omega(2^{-\lambda}\epsilon)$	$k \approx \frac{k'}{3} - \frac{\lambda}{3}$
(d) [JP14a]	Simulating Auxiliary Inputs	$O\left(t \cdot 2^{3\lambda}\epsilon^{-2} + 2^{4\lambda}\epsilon^{-2}\right)$	$\Omega(\epsilon)$	$k \approx \frac{k'}{4} - \lambda$
(e) [VZ13]	Simulating Auxiliary Inputs	$\Omega\left(s \cdot 2^{\lambda}\epsilon^{-2} + 2^{\lambda}\epsilon^{-4}\right)$	$\Omega(\epsilon)$	$k \approx \frac{k'}{5} - \frac{\lambda}{5}$
(f) [GW11]	Relaxed HILL Entropy	$O\left(s \cdot 2^{\lambda}\epsilon^{-2} - 2^{2\lambda}\epsilon^{-2}\right)$	$\Omega(\epsilon)$	$k \approx \frac{k'}{3} - \frac{2}{3}\lambda$
(g) [PS15]	Average Metric Entropy	$O\left(s \cdot 2^{\lambda}\epsilon^{-2} - 2^{2\lambda}\right)$	$\Omega(\epsilon)$	$k \approx \frac{k'}{3} - \frac{\lambda}{3}$

Table : Qualitative bounds on chain rules for HILL entropy. To compare different chain rules, we consider a (t', ϵ')-secure weak PRF where $t'/\epsilon' = 2^{k'}$ (for any choice of of t'), then after λ bits of leakage on the key, the PRF is $t/\epsilon = 2^k$ secure (for any choice of t), where depending on the chain rule used, k can take the values as indicated in the table.

Leakage-resilient stream ciphers comparison

Cipher	Analysis	Proof techniques	$t' =$	$\epsilon' =$	Security Level **our contribution**	Comments/Restrictions
(1)	[Pie09]	Pseudoentropy chain rules	$t \cdot \mathrm{poly}(\epsilon^{-1}, 2^{\lambda})$	$\mathrm{poly}(\epsilon, 2^{-\lambda})$	$k \ll \frac{1}{8}k'$	large number of blocks
(1)	[JP14b]	Aux. Inputs Simulator	$O\left(t \cdot 2^{4\lambda}\epsilon^{-4}\right)$	$\Omega\left(2^{-2\lambda}\epsilon\right)$	$k \approx \frac{k'}{6} - \frac{5}{6}\lambda$	
(1)	[VZ13]	Aux. Inputs Simulator	$O\left(t \cdot 2^{\lambda}\epsilon^{-2} + \epsilon^{-4}\right)$	$\Omega\left(2^{-2\lambda}\epsilon\right)$	$k \approx \frac{k'}{6} - \frac{1}{3}\lambda$	
(1)	Dream bound	Aux. Inputs Simulator	$O\left(t \cdot 2^{3\lambda}\epsilon^{-2}\right)$	$\Omega\left(2^{-2\lambda}\epsilon\right)$	$k \approx \frac{k'}{4} - \lambda$	unproven (a flaw in [JP14b])
(2)	[FPS12]	Pseudoentropy chain rules	$O\left(t \cdot 2^{4\lambda}\epsilon^{-4}\right)$	$\Omega\left(2^{-2\lambda}\epsilon\right)$	$k \approx \frac{k'}{5} - \frac{6}{5}\lambda$	large public seed
(3)	[YS13]	Square-friendly apps.	$O\left(t \cdot \epsilon^{-2}\right)$	$\Omega\left(2^{-3\lambda}\epsilon^{2}\right)$	$k \approx \frac{k'}{4} - \frac{3}{4}\lambda$	only in minicrypt

Table : Different bounds for wPRF-based leakage-resilient stream ciphers. The underlying weak PRF(s) has k' bits of security, and the cipher has k bits of security, understood in terms of the time-success ratio. The numbers denote: (1) The EUROCRYPT'09 cipher, (2) The CSS'10/CHES'12 cipher, (3) The CT-RSA'13 cipher. The dream bound refers to better bounds claimed in [JP14b] which remain unproven because of a subtle flaw [Pie].

Security of weak pseudo-random functions with weak keys

Bound	Analysis	Proof techniques	$t' =$	$\epsilon' =$	Security Loss **our contribution**	Comments/Restrictions
(a)	[Pie09]	Pseudoentropy chain rules	$O\left(t \cdot \epsilon^{-2}\right)$	$\Omega\left(2^{-\lambda}\epsilon\right)$	$k \approx \frac{k'}{3} - \frac{1}{3}\lambda$	large number of queries
(b)	[DY13]	Square-security	$O\left(t\right)$	$\Omega\left(2^{-\lambda}\epsilon^2\right)$	$k' \approx \frac{k}{2} - \frac{1}{2}\lambda$	

Table : Different bounds for wPRFs with weak keys. A weak PRF which has k' bits of security with the uniform keys, has k bits of security for keys with entropy deficiency λ.

Plan

Conclusions

- We provide a clear formula on security loss
- We give a quantitative survey of bounds for pseudoentropy chain rules, leakage-resilient stream ciphers, and security of weak pseudorandom functions with weak keys

References

- Stefan Dziembowski and Krzysztof Pietrzak, Leakage-resilient cryptography, Proceedings of the 2008 49th Annual IEEE Symposium on Foundations of Computer Science (Washington, DC, USA), FOCS '08, IEEE Computer Society, 2008, pp. 293–302.
- Yevgeniy Dodis and Yu Yu, Overcoming weak expectations, Theory of Cryptography (Amit Sahai, ed.), Lecture Notes in Computer Science, vol. 7785, Springer Berlin Heidelberg, 2013, pp. 1–22 (English).
- Benjamin Fuller, Adam O'Neill, and Leonid Reyzin, A unified approach to deterministic encryption: New constructions and a connection to computational entropy, J. Cryptology **28** (2015), no. 3, 671–717.
- Sebastian Faust, Krzysztof Pietrzak, and Joachim Schipper, Practical leakage-resilient symmetric cryptography, Cryptographic Hardware and Embedded Systems – CHES 2012 (Emmanuel Prouff and Patrick Schaumont, eds.), Lecture Notes in Computer Science, vol. 7428, Springer Berlin Heidelberg, 2012, pp. 213–232 (English).
- Craig Gentry and Daniel Wichs, Separating succinct non-interactive arguments from all falsifiable assumptions, Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing (New York, NY, USA), STOC '11, ACM,