Randomness in Cryptography	April 18, 2013

Lecture 14: Robust Extractors and Their Limitations

Lecturer: Yevgeniy Dodis *Scribe: Umut Orhan*

1 Robust Extractors

How to authenticate the seed S? As a motivating example it might be instructive to think about following two scenarios:

1. one-party "remembers" secret X and stores public S to help extract $R = \mathsf{Ext}(X; S)$ (many times)
   - where to store S?
   - what if S is modified to $\tilde{S} \neq S$ ($\tilde{R} = \mathsf{Ext}(X; \tilde{S})$ could be correlated to R)
2. $\underset{S \leftarrow \$}{A(X)} \xrightarrow{S} \underset{Eve}{\Big|} \xrightarrow{\tilde{S}} B(X)$ (a type of attack)

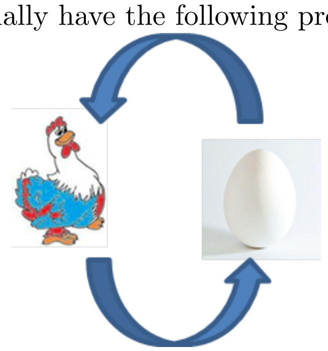
Question 1 *Can we "authenticate" S?*

- *using what? X itself!*

Good news: can authenticate S using weak X if $K = \mathbf{H}_\infty(X) \leq \frac{n}{2}$ $(n = |X|)$

Bad news: need $k > \frac{n}{2}$

Worse news: even for $k > \frac{n}{2}$ have circularity
We essentially have the following problem



$T = \mathsf{Tag}_X(S), R = \mathsf{Ext}(X; S)$

- maybe T leaks info about R
- maybe R helps forge T

Syntax: $(\mathsf{Gen}, \mathsf{Rep})$, where Gen corresponds to generation and Rep corresponds to reproduction

- $\mathsf{Gen}(X; S) = (\underbrace{R}_{\text{extracted key}}, \underbrace{P}_{\text{public helper}})$, where $R \in \{0,1\}^m$.
  (sometimes call $R = \mathsf{Ext}(X; S)$, $P = \mathsf{Auth}(X; S)$)
- $\mathsf{Rep}(X; \tilde{P}) = \tilde{R} \in \{0,1\}^m \cup \{\perp\}$
  (sometimes call $\mathsf{Ver}(X; P) = [\mathsf{Rep}(X; P) \overset{?}{\neq} \perp])$)
- Correctness requirement: $P = \tilde{P} \Rightarrow R = \tilde{R}$

2 Security

3 parameters for security

- $K = \mathbf{H}_\infty X$ min-entropy
- ε extraction security
- δ authentication security

Define (K, ε, δ)-robust extractor

2.1 Extraction security

$\mathsf{SD}(R; U_m | P) \le \varepsilon$ (note before conditioned on S)

2.2 Authentication Security (Robustness)

Attempt 1 (Definition 1): $\forall K$-source X, $\forall A$, $\mathsf{Adv}(A) \le \delta$, where $S \leftarrow \$$ and A corresponds to attacker. $\mathsf{Gen}(X; S) = (R, P)$, $A(P) \to \tilde{P}$, A wins if $\mathsf{Rep}(X; \tilde{P}) \notin \{R, \perp\}$.

This attempt is problematic. Because R vs $\perp$ decision potentially leaks info about X and might kill "composition".

Artificial Counter Example: $\mathsf{Gen}X; S$: $\mathsf{Gen}'(X; S) \leftarrow (R', P')$ set $R = R'$, $P = (P', 0, 0)$ and $\mathsf{Rep}'(X; (\tilde{R}', \underbrace{i}_{\text{index}}, \underbrace{b}_{\text{bit}}))$: if $X_i > 0 \& X_i = b$ output $\perp$, else $\mathsf{Rep}(X; \tilde{P})$ Claim $(\mathsf{Gen}', \mathsf{Rep}')$ satisfies Definition 1 but horrible for repeated use (can learn X).

Attempt 2 (Definition 2, Pre-application Robustness): Same as Attempt 1, but attacker wins if $\tilde{P} \neq P$ and $\mathsf{Rep}(X; \tilde{P}) \neq \perp$

"**Composition**": $A^{\mathsf{Rep}(X;\cdot)}$ can't cause $\tilde{R} \in \{R, \perp\}$.

Definition 1 $\not\Rightarrow$ composition

Definition 2 $\not\Rightarrow$ "strong" composition, t attempts $\Rightarrow \Pr(\text{breaking}) \le t\delta$

Attempt 3 (Definition 3, Post-application Robustness): $S \leftarrow \$ \, (R,P) \leftarrow \mathsf{Gen}(X;S), A(R,P) \rightarrow \tilde{P}$
Win: $\tilde{P} = P$ and $\mathsf{Rep}(X;P) \neq \perp$. $\Pr(\text{win}) \leq \delta$

Idea 1: Set $P = (S,T)$, $R = \mathsf{Ext}(X;S)$
$T = \mathsf{Tag}_X(S) \leftarrow$ MAC with weak X (so $k > \frac{n}{2}$). Reject if Tag fails else run Extractor.

$$h(X;S) = (R,T) = (\mathsf{Ext}(X;S), \mathsf{Tag}_X(S))$$

-Essentially, A gets $f(X;S)$ in both ext/auth experiments.

For extraction security; it is enough if $h(X;S)$ is extractor with seed S (universality with key S)
For authentication security; it is enough if $h(X;S)$ is pairwise independent with key X
Is there an h satisfying both?

$$h(\underbrace{X}_{\text{pairwise independent}}, \underbrace{S}_{\text{universal}})$$

$$x = (a,b), \qquad |a| = |b| = |s| = \frac{n}{2}, \qquad h((a,b),s) = as + b$$

Claim 1: h is universal keyed by S.

$$\forall (a,b) = (a',b'), \quad \Pr_S(aS + b = a'S + b') = \Pr_S((a-a')S = b - b') = \begin{cases} 0, & \text{if } a = a', b \neq b' \\ 2^{-n/2}, & \text{if } a \neq a' \end{cases}$$

Claim 2: $\forall s \neq \tilde{s}, (A\tilde{s} + B | As + B) \equiv (U_{n/2} | As + B)$. Let $Y = h(X;S) = AS + B$.
How to split Y into (R,T)?
-Set $|R| = m < \frac{n}{2}$, $|T| = \frac{n}{2}] - m$ and calculate ε, σ.

Extraction:

$$\begin{aligned} (R,P) = (R,(T,S)) \equiv (\underbrace{(R,T)}_{Y}, S) \underset{\varepsilon'}{\approx} (U_{n/2}, S) &\equiv (U_m, (U_{n/2-m}, S)) \\ &\underset{\varepsilon'}{\approx} (U_m, \underset{\text{truncation of } AS+B}{\overset{}{\underset{\shortparallel}{(T,S)}}}) \\ &\equiv (U_m, P), \end{aligned}$$

where $\varepsilon' \overset{\text{LHL}}{\overset{\downarrow}{=}} \frac{1}{2}\sqrt{2^{\frac{n}{2}-k}}$.

$$\varepsilon = 2\varepsilon' = \sqrt{2^{nfrm-e-k}} \Rightarrow k \geq \frac{n}{2} + 2\log\frac{1}{\varepsilon} \tag{1}$$

Authentication (Post-Robustness): $\delta = \delta' 2^{n-k}$, where δ'-security with uniform $X \equiv U_n$. What is δ'?

$$A(R, P) \to \tilde{P} = (\tilde{S}, \tilde{T}) \neq (S, T)$$

If $\tilde{S} = S \Rightarrow A$ lost as $\tilde{T}$ won't match.
So assume $\tilde{S} \neq S$, then by pairwise independence to learn $AS + B$,

$$\Pr(\text{can predict } [A\tilde{S} + B]_{\frac{n}{2}-m}) \leq 2^{m-\frac{n}{2}} \Rightarrow \delta' \leq 2^{m-n/2}$$

$$\delta = \delta' * 2^{n-k} = 2^{m-n/2+n-k} = 2^{m+n/2-k}$$

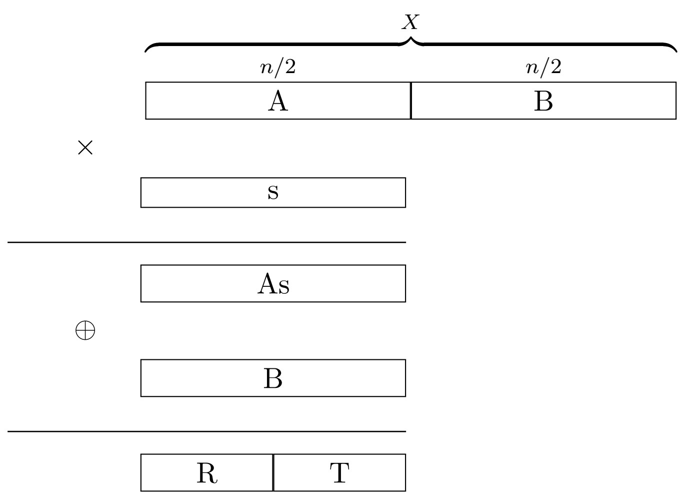
$$\Updownarrow$$

$$k \leq \frac{n}{2} + m + \log\frac{1}{\delta}$$

$$\Updownarrow$$

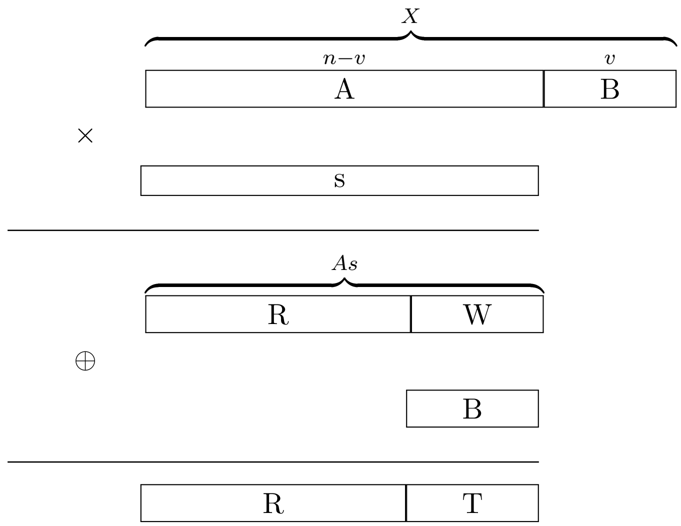
$$m \leq k - \frac{n}{2} - \log\frac{1}{\delta} \tag{2}$$

Theorem 1 *$\forall \varepsilon \delta$ and $\forall k > \frac{n}{2} + \max(2\log\frac{1}{\varepsilon}, \log\frac{1}{\delta})$, $\exists (k, \varepsilon, \delta)$-post-application robust extractor with output length $m = k - \frac{n}{2} - \log\frac{1}{\delta}$.*



B was added to both R (post-application, not needed for extraction) and T.

New idea:



$$n = m + 2v, v = \frac{n-m}{2}$$

-R already universal, for extraction this is enough.
-only T is pairwise independent.

New pre-application: Let $v = \frac{n-m}{2}(m = n - 2v), Gen(X;S) : X = (A,B), |B| = v, |A| = n - v$,

$$S \xleftarrow{\$} GF[2^{n-v}].$$

Let $Y = AS, R = [Y]^m, W = [Y]_{m+1}^{n-v}, T = W \oplus B, P = (S,T)$
$\mathsf{Rep}((A,B),(\tilde{S},\tilde{T}))$ check if $\tilde{T}$ is correct if so extract.

Extraction security:

$$\varepsilon = 2\varepsilon' = \sqrt{2^{n-v-k}} = \sqrt{2^{n-\frac{n-m}{2}-k}} = \sqrt{2^{\frac{n}{2}+\frac{m}{2}-k}}$$

$$k \geq \frac{n}{2} + \frac{m}{2} + 2\log\frac{1}{\varepsilon} \quad (\text{previously amp. } k \geq \frac{n}{2} + \log\frac{1}{\varepsilon})$$

Authentication: $\delta = 2^{n-k}$. $\delta' = 2^{n-k-v} = 2^{n-k-\frac{n-m}{2}} = 2^{\frac{n}{2}+\frac{m}{2}-k}$

$$k \geq \frac{n}{2} + \frac{m}{2} + \log\frac{1}{\delta} \quad (\text{amp. } k \geq \frac{n}{2} + m + \log\frac{1}{\delta})$$

$\tilde{m} = 2(\frac{n}{2} - k - \max(2\log\frac{1}{\varepsilon}, \log\frac{1}{\delta})$ twice as large if $\log\frac{1}{\delta} > 2\log 1\varepsilon$.

Theorem 2 *$\forall\varepsilon,\delta,\forall k \geq \frac{n}{2} + \max(2\log\frac{1}{\varepsilon}, \log\frac{1}{\delta})$ pre-app with $m = 2(k - \frac{n}{2} - \max(2\log\frac{1}{\varepsilon}, \log\frac{1}{\delta}))$. Almost twice as much, but same k.*

We can pose two interesting questions,

Question 2 *Is $k > \frac{n}{2}$ essential? (YES)*

Question 3 *Is $k > \frac{n}{2}$] essential for probab. MACs w/ weak keys? (YES)*

Lemma 1 *$\forall$ randomized $\mathsf{Auth} : \{0,1\}^n \to \{0,1\}^t$, $\mathsf{Ver} : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}$, $\forall \rho$ (we'll use $\rho = 1$), at least one pf the following holds:*

(1) $\exists (n,k)$-source X s.t. $\Pr_{\text{coins of Auth}}(\mathsf{Ver}(X, \mathsf{Auth}(X)) < \rho$
(2) $\exists (n,k)$-source X and $P \in \{0,1\}^t$ s.t. $\Pr(\mathsf{Ver}(X,P) = 1) > \frac{\rho}{2}$
(3) $\exists (n,k)$-source X s.t. $\mathbf{H}_\infty(X|\mathsf{Auth}(X)) \leq \max(0, 2k-n) + \log \frac{1}{\rho} + 2$

Corollary 2 *For $\rho = 1$ and perfect correctness, either $\exists X$ fixed p s.t. $\Pr(\mathsf{Ver}(X,p) = 1) > \frac{1}{2}$ or $\exists X$ s.t. $\mathbf{H}_\infty(X, \mathsf{Auth}(X)) \leq 2 + \max(0, 2k-n)$, if $k \leq \frac{n}{2}$, $\mathbf{H}_\infty(X|\mathsf{Auth}(X)) \leq 2$. Proof is at Appendix C of [2].*

Corollary 3 *$\forall (k, \varepsilon, \delta)$ pre-application robust extractor with key length $m \geq 4$, $\varepsilon < \frac{1}{16}$, $\delta < \frac{1}{2}$ must have $k > \frac{n}{2}$ and $|P| \geq n - k - 2$*

Corollary 4 *$\forall$ even probabilistic (k, δ) secure MAC (even for 1 bit) where $\delta < \frac{1}{4}$ must have $k > \frac{n}{2}$ and $|T| \geq n - k - 2$.*

Proof: $\mathsf{Auth}(X) = \mathsf{Tag}_X(0)$
cond(2) $\Rightarrow$ can forge $\mathsf{Tag}_X(0)$ w/ pr$> \frac{1}{2}$
cond(3) $\Rightarrow$ can forge $\mathsf{Tag}_X(1)|\mathsf{Tag}_X(0)$ w/ pr$> \frac{1}{4}$

$\square$

open problem: $k > \frac{n}{2}$ prove upper band on m. (almost sloved for pre-app, how about post-app?)

Computational Robust Extractors? Can we beat $k > \frac{n}{2}$, if A for robustness is computationally bounded? -Yes in RO model.[1] Set $R = \mathsf{Ext}(X; S)$, $T = H(X, S)$, H-random oracle (X is independent of H)

Intuition: $\mathbf{H}_\infty(X|R)$-high and T doesn't help unless A queries $H(X,S)$. Hence $\forall \tilde{s} \neq s$ hard to predict $H(X, \tilde{s}$.

$$\delta = q\mathsf{pred}(X|R,S) = q2^{m-k}, \qquad m = k - \max(2 \log 1\varepsilon, \log q) \forall k$$

Big open question: Instantiate H? -Idea 1: get rid of "weak" X by $\mathsf{Ext}(X; S) = (R, k)$, $T = \mathsf{Tag}_k(S)$. Now $s \to \tilde{s}$, $k \to \tilde{k}$ related key Tag.

References

[1] Boyen, X., Dodis, Y., Katz, J., Ostrovsky, R., & Smith, A. (2005). Secure remote authentication using biometric data. In Advances in CryptologyEUROCRYPT 2005 (pp. 147-163). Springer Berlin Heidelberg.

[2] Dodis, Y., & Wichs, D. (2009, May). Non-malleable extractors and symmetric key cryptography from weak secrets. In Proceedings of the 41st annual ACM symposium on Theory of computing (pp. 601-610). ACM.

[3] Dodis, Y., Katz, J., Reyzin, L., & Smith, A. (2006). Robust fuzzy extractors and authenticated key agreement from close secrets. In Advances in Cryptology-CRYPTO 2006 (pp. 232-250). Springer Berlin Heidelberg.