Generalized Special Soundness

Parsa

December 16, 2024

Abstract

Keywords:

Contents

[TODO:

- **Formal definition of k-SS, gamma-SS, prob-SS.**
- **A theorem saying that Kilian is k-SS iff gamma-SS, with precise tradeoff.**
- **A theorem saying that Kilian is k-SS/gamma-SS when PCP has deterministic extractor.**
- **A theorem (a counterexample, concrete PCP with probabilistic extractor) saying that resulting Kilian is not k-SS/gamma-SS.**

—Ziyi]

2: lemma 2.9 , theorem 2.10
3: -
4: lemma 2.7,

1 Preliminaries

1.1 Probabilistic Chekable proofs

A probabilistically checkable proof system (PCP for short) denoted by (P, V) is a proof system where the probabilistic verifier V has oracle access to the proof string Π generated by the prover P.

Definition 1.1 (PCP completeness)**.** *A PCP (P, V) for relation R has completeness error δ if, for every pair $(\mathbb{x}, \mathbb{w}) \in R$:*

$$\Pr\left[V^{\Pi}(\mathbb{x}; \rho) = 1 \mid \Pi \leftarrow P(\mathbb{x}, \mathbb{w}), \rho \leftarrow \{0,1\}^r\right] \geq 1 - \delta(|\mathbb{x}|)$$

Definition 1.2 (PCP soundness)**.** *A PCP (P, V) for relation R has soundness error ε if, for every (unbounded) circuit $\tilde{P}$ and auxiliary input distribution D:*

$$\Pr\left[\begin{array}{c} |\mathbb{x}| \leq n \\ \mathbb{x} \notin L[R] \\ V^{\tilde{\Pi}}(\mathbb{x}; \rho) = 1 \end{array} \middle| \begin{array}{l} (\mathbb{x}, \tilde{\Pi}) \leftarrow \tilde{P} \\ \rho \leftarrow \{0,1\}^r \end{array}\right] \leq \varepsilon(n)$$

Some PCPs have a stronger notion of soundness called knowledge soundness, these PCPs are called PCP of knowledge.

Definition 1.3 (PCP of knowledge)**.** *A PCP (P, V) for relation R has knowledge soundness error κ if there is an efficient algorithm E that, for every (unbounded) circuit $\tilde{P}$:*

$$\Pr\left[\begin{array}{c} |\mathbb{x}| \leq n \\ (\mathbb{x}, \mathbb{w}) \notin R \\ V^{\tilde{\Pi}}(\mathbb{x}; \rho) = 1 \end{array} \middle| \begin{array}{c} (\mathbb{x}, \tilde{\Pi}) \leftarrow \tilde{P} \\ \rho \leftarrow \{0,1\}^r \\ \mathbb{w} \leftarrow E(\mathbb{x}, \tilde{P}i) \end{array}\right] \leq \kappa(n)$$

Intuitively when V and E are parts of a knowledge sound PCP, probability of a proof string $\tilde{\Pi}$ convincing the verifier and not admitting a witness is low. We can define a new and stronger definition called α-knowledge soundness. Intuitively when V and E are parts of a α-knowledge sound PCP and $\tilde{\Pi}$ is a proof string convincing V with high probability then it also admits a witness with high probability.

Definition 1.4 (α-knowledge soundness)**.** *For any function $\alpha\colon \mathbb{N} \to [0,1]$. A PCP (P, V) for relation R has α-knowledge soundness error κ_α if there is an efficient algorithm E that, for every (unbounded) circuit $\tilde{P}$ and $\mathbb{x} \in \{0,1\}^n$:*

$$\Pr\left[V^{\tilde{\Pi}}(\mathbb{x};\rho) = 1 \middle| \begin{array}{c} (\mathbb{x},\tilde{\Pi}) \leftarrow \tilde{P} \\ \rho \leftarrow \{0,1\}^r \end{array}\right] > \kappa_\alpha(n) \Rightarrow \Pr\left[(\mathbb{x},\mathbb{w}) \notin R \middle| \ (\mathbb{x},\tilde{\Pi}) \leftarrow \tilde{P}\ \right] \le \alpha(n)$$

Lemma 1.5. *Any α-knowledge sound PCP with α-knowledge error κ_α is knowledge sound with knowledge error bounded by $\kappa_\alpha + \alpha$.*

Proof. Any extractor E satisfying the bound for α-knowledge soundness also satisfies the bound for knowledge soundness.

$$\begin{aligned}
&\Pr\left[\begin{array}{c} (\mathbb{x},\mathbb{w}) \notin R \\ V^{\tilde{\Pi}}(\mathbb{x};\rho) = 1 \end{array} \middle| \begin{array}{c} (\mathbb{x},\tilde{\Pi}) \leftarrow \tilde{P} \\ \rho \leftarrow \{0,1\}^r, \mathbb{w} \leftarrow E(\mathbb{x},\tilde{\Pi}) \end{array}\right] \\
&\le \Pr\left[\begin{array}{c} (\mathbb{x},\mathbb{w}) \notin R \\ V^{\tilde{\Pi}}(\mathbb{x};\rho) = 1 \\ Win_{\mathbb{x}}(\tilde{\Pi}) < \kappa_\alpha(|\mathbb{x}|) \end{array} \middle| \begin{array}{c} (\mathbb{x},\tilde{\Pi}) \leftarrow \tilde{P} \\ \rho \leftarrow \{0,1\}^r \\ \mathbb{w} \leftarrow E(\mathbb{x},\tilde{\Pi}) \end{array}\right] + \Pr\left[\begin{array}{c} (\mathbb{x},\mathbb{w}) \notin R \\ V^{\tilde{\Pi}}(\mathbb{x};\rho) = 1 \\ Win_{\mathbb{x}}(\tilde{\Pi}) \ge \kappa_\alpha(|\mathbb{x}|) \end{array} \middle| \begin{array}{c} (\mathbb{x},\tilde{\Pi}) \leftarrow \tilde{P} \\ \rho \leftarrow \{0,1\}^r \\ \mathbb{w} \leftarrow E(\mathbb{x},\tilde{\Pi}) \end{array}\right] \\
&\le \Pr\left[V^{\tilde{\Pi}}(\mathbb{x};\rho) = 1 \middle| \begin{array}{c} (\mathbb{x},\tilde{\Pi}) \leftarrow \tilde{P} \\ \rho \leftarrow \{0,1\}^r \\ \mathbb{w} \leftarrow E(\mathbb{x},\tilde{\Pi}) \\ Win_{\mathbb{x}}(\tilde{\Pi}) < \kappa_\alpha(|\mathbb{x}|) \end{array}\right] + \Pr\left[(\mathbb{x},\mathbb{w}) \notin R \middle| \begin{array}{c} (\mathbb{x},\tilde{\Pi}) \leftarrow \tilde{P} \\ \rho \leftarrow \{0,1\}^r \\ \mathbb{w} \leftarrow E(\mathbb{x},\tilde{\Pi}) \\ Win_{\mathbb{x}}(\tilde{\Pi}) \ge \kappa_\alpha(|\mathbb{x}|) \end{array}\right] \\
&\le \kappa_\alpha(|\mathbb{x}|) + \alpha(|\mathbb{x}|)
\end{aligned}$$

□

Lemma 1.6. *Any knowledge sound PCP with knowledge error κ and deterministic extractor is α-knowledge sound with $\alpha = 0$ and $\kappa_\alpha \le \kappa$.*

Proof. Assume $\Pr\left[V^{\tilde{\Pi}}(\mathbb{x};\rho) = 1 \mid \tilde{\Pi} \leftarrow \tilde{P(\mathbb{x})}\right] > \kappa(|\mathbb{x}|)$.
By definition $\Pr\left[\begin{array}{c} V^{\tilde{\Pi}}(\mathbb{x};\rho) = 1 \\ (\mathbb{x},\mathbb{w}) \notin R \end{array} \middle| \begin{array}{c} \tilde{\Pi} \leftarrow \tilde{P(\mathbb{x})} \\ \mathbb{w} \leftarrow E(\mathbb{x},\tilde{\Pi}) \end{array}\right] \le \kappa(|\mathbb{x}|)$. Since the PCP extractor is deterministic, it suffices to only consider the case $(\mathbb{x},\mathbb{w}) \notin R$.

$$\Pr\left[\begin{array}{c} V^{\tilde{\Pi}}(\mathbb{x};\rho) = 1 \\ (\mathbb{x},\mathbb{w}) \notin R \end{array} \middle| \begin{array}{c} \tilde{\Pi} \leftarrow \tilde{P(\mathbb{x})} \\ \mathbb{w} \leftarrow E(\mathbb{x},\tilde{\Pi}) \end{array}\right] = \Pr\left[V^{\tilde{\Pi}}(\mathbb{x};\rho) = 1 \middle| \begin{array}{c} \tilde{\Pi} \leftarrow \tilde{P(\mathbb{x})} \\ \mathbb{w} \leftarrow E(\mathbb{x},\tilde{\Pi}) \end{array}\right] \cdot \Pr\left[(\mathbb{x},\mathbb{w}) \notin R \middle| \begin{array}{c} \tilde{\Pi} \leftarrow \tilde{P(\mathbb{x})} \\ \mathbb{w} \leftarrow E(\mathbb{x},\tilde{\Pi}) \\ V^{\tilde{\Pi}}(\mathbb{x};\rho) = 1 \end{array}\right]$$

$$\Rightarrow \Pr\left[V^{\tilde{\Pi}}(\mathbb{x};\rho) = 1 \middle| \begin{array}{c} \tilde{\Pi} \leftarrow \tilde{P(\mathbb{x})} \\ \mathbb{w} \leftarrow E(\mathbb{x},\tilde{\Pi}) \end{array}\right] \le \frac{\kappa(|\mathbb{x}|)}{\Pr\left[(\mathbb{x},\mathbb{w}) \notin R \middle| \begin{array}{c} \tilde{\Pi} \leftarrow \tilde{P(\mathbb{x})} \\ \mathbb{w} \leftarrow E(\mathbb{x},\tilde{\Pi}) \\ V^{\tilde{\Pi}}(\mathbb{x};\rho) = 1 \end{array}\right]} \le \kappa(|\mathbb{x}|).$$

Which is a contradiction with the assumption. □

1.2 Interactive proofs

An interactive proof system (IP for short) denoted by (P, V) is a proof system where the probabilistic verifier V interacts with the prover P and at the end of their interaction, V either accepts or rejects.
When the prover is considered to be computationally bounded to polynomial computations, the proof system is called an interactive argument.

Definition 1.7 (k-special soundness). *An interactive proof system (P, V) is k-special sound if, there is an efficient algorithm E such that for any $\mathbb{x} \in \{0,1\}^n$ and set $T = (\tau, r_i, z_i)_{i\in[k]}$ of accepting transcripts for $\mathbb{x}$ with the same first message and different challenges ($i \neq j \rightarrow r_i \neq r_j$), $\mathbb{w} = E(\mathbb{x}, T)$ is a valid witness for $\mathbb{x}$ with probability 1.*

Definition 1.8 (Monotone structure). *Let C be a set, $\Gamma \subseteq 2^C$ is a monotone structure if for any $X \subseteq Y \subseteq C$, $X \in \Gamma \rightarrow Y \in \Gamma$. This monotone structure is denoted by (Γ, C).*

Definition 1.9 (Γ-special soundness). *Let $(\Gamma, \{0,1\}^r)$ be a monotone structure. An interactive proof (P, V) is Γ-special sound if there is an efficient algorithm E that for any instance $\mathbb{x}$ and set of accepting transcripts $T = (\tau, r_i, z_i)_{i\in[k]}$ for $\mathbb{x}$, such that $\{r_1, r_2, ..., r_k\} \in \Gamma$, $\mathbb{w} \leftarrow E(\mathbb{x}, T)$ is a valid witness for $\mathbb{x}$ with probability 1.*

Definition 1.10 ((k, g)-special soundness). *Let (P, V) be an interactive proof. M denotes the set of possible first messages and C the set of possible challenges. A predicate is a function $g\colon M \times (C \times \{0,1\}^*)^* \rightarrow \{0,1\}$ that assigns a bit to a set of (possibly partial) transcripts with the same first message. Additionaly if $g(\tau, (r_i, z_i)_{i\in[k]}) = 1$ for some $k \in \mathbb{N}$, then for any set $A \subseteq [k]$, $g(\tau, (r_i, z_i)_{i\in A}) = 1$.*
Let Consistent$_k$ be the set of all transcripts $T \in M \times (R \times \{0,1\}^*)^k$ such that $g(T) = 1$.

An interactive proof system (P, V) is (k, g)-special sound if, there is an efficient algorithm E such that for any $T \in$ Consistent$_k$ where all r_i are different, $\mathbb{w} = E(\mathbb{x}, T)$ is a valid witness for $\mathbb{x}$ with probability 1.

Lemma 1.11. *Any k-special sound proof is also (k, g)-special sound when g is the predicate that indicates all transcripts are accepting.*

Definition 1.12 (Q-admissible distribution). *A distribution D_k on a set Ω^k is Q-admissible when there exists a negligible function $\epsilon(\lambda)$ and an algorithm $Samp^{O_\Omega}$ with access to a random oracle O_Ω taking uniformly random samples from Ω such that:*

- *The output of $Samp$ is $\epsilon(\lambda)$-close to D_k.*
- *$Samp$ in expectation makes $Q(\lambda)$ many queries to O_Ω.*
- *$Samp$ works as follows: Let $(r_1, r_2, ..., r_t)$ be the result of all queries of $Samp$ to O_Ω. $Samp$ computes an index set $(i_1, i_2, ..., i_k)$ and its output is $(r_{i_1}, r_{i_2}, ..., r_{i_k})$. Notice that $Samp$ is free to use inefficient computations for computing the index set.*

Definition 1.13 (Admissible distribution). *A distribution D_k on a set Ω^k is admissible when there exists a polynomial $Q(\lambda)$ such that D_k is Q-admissible.*

Definition 1.14 ((k, g)-probabilistic special soundness). *An interactive proof (P, V) with randomness space Ω is (k, g)-probabilistic special sound if there exists an efficient algorithm E such that for any distribution D supported on Consistent$_k$ and admissible marginal distribution on Ω^k we have:*

$$\Pr\left[\begin{array}{c} \mathbb{w} \leftarrow E(\tau, (r_i, z_i)_{i\in[k]}) \\ (\mathbb{x}, \mathbb{w}) \in R \end{array}\right] = 1 - negl(\lambda).$$

Intuitively (k, g)-probabilistic special soundness means that the extractor doesn't succeed for all transcript sets in Consistent_k but it does succeed with high probability on transcripts whose challenges are approximately randomly sampled. In other words, we can assume that with high probability the challenges in a given transcript are chosen from a poly-bounded set of random challenges.

2 Special Soundness of Kilian's protocol

In this section we look at how interactive arguments created using Kilian's protocol fit into notions of special soundness. Through out this section let VC be the vector commitment scheme used by Kilian, and position binding error of VC denoted by ε_{VC}

2.1 Kilian's protocol is not Γ-special sound

Lemma 2.1. *If there exists a knowledge sound PCP (P, V) for relation R with knowledge error κ and extractor E, then there exists a PCP (P', V') with knowledge error $\kappa + \frac{k}{2^r}$ that is not k-special sound after compilation with Kilian.*

Proof. Let A be an arbitrary set of size k in $\{0, 1\}^r$, define P' and V' as follows:
P' :

1. Simulate P and get proof string Π.
2. Output $\Pi' = \perp \| \Pi$.

V' :

1. V' is given randomness $\rho \in \{0, 1\}^r$.
2. If $\rho \in A$ make all queries to the first location in the proof string and accept regardless of the answers.
3. If $\rho \notin A$ simulate V.

First we shall prove that (P', V') has knowledge error bounded by $\kappa + \frac{k}{2^r}$.

$$\Pr\left[\begin{array}{c} V'^{\tilde{\Pi}}(\mathbb{x}; \rho) = 1 \\ (\mathbb{x}, \mathbb{w}) \notin R \end{array} \middle| \begin{array}{c} \tilde{\Pi} \leftarrow P \\ \mathbb{w} \leftarrow E(\tilde{\Pi}) \end{array}\right] = \Pr\left[\begin{array}{c} \rho \in A \\ V'^{\tilde{\Pi}}(\mathbb{x}; \rho) = 1 \\ (\mathbb{x}, \mathbb{w}) \notin R \end{array} \middle| \begin{array}{c} \tilde{\Pi} \leftarrow P \\ \mathbb{w} \leftarrow E(\tilde{\Pi}) \end{array}\right] + \Pr\left[\begin{array}{c} \rho \notin A \\ V^{\tilde{\Pi}}(\mathbb{x}; \rho) = 1 \\ (\mathbb{x}, \mathbb{w}) \notin R \end{array} \middle| \begin{array}{c} \tilde{\Pi} \leftarrow P \\ \mathbb{w} \leftarrow E(\tilde{\Pi}) \end{array}\right]$$

$$\leq \Pr\left[\begin{array}{c} V^{\tilde{\Pi}}(\mathbb{x}; \rho) = 1 \\ (\mathbb{x}, \mathbb{w}) \notin R \end{array} \middle| \begin{array}{c} \tilde{\Pi} \leftarrow P \\ \mathbb{w} \leftarrow E(\tilde{\Pi}) \end{array}\right] + \Pr[\rho \in A] \leq \kappa + \frac{k}{2^r}$$

Now we shall prove that (P', V') is not k-special sound after compilation with Kilian. Any accepting transcript set with challenges in A carries 0 information therefore it is not possible that some efficient algorithm can compute a valid witness given such a transcript set unless $R \in P$. $\square$

Lemma 2.2. *Let $(\Gamma, \{0, 1\}^r)$ be a monotone structure such that the smallest set in Γ has size k, if there exists a knowledge sound PCP (P, V) for relation R with knowledge error κ and extractor E, then there exists a PCP (P', V') with knowledge error $\kappa + \frac{k}{2^r}$ that is not Γ-special sound after compilation with Kilian.*

Proof. Let A be some set in Γ, define P' and V' as follows:
P' :

1. Simulate P and get proof string Π.

2. Output $\Pi' = \perp \| \Pi$.

V' :

1. V' is given randomness $\rho \in \{0,1\}^r$.

2. If $\rho \in A$ make all queries to the first location in the proof string and accept regardless of the answers.

3. If $\rho \notin A$ simulate V.

First we shall prove that (P', V') has knowledge error bounded by $\kappa + \frac{k}{2^r}$.

$$\Pr\left[\begin{array}{c} V'^{\tilde{\Pi}}(\mathbb{x};\rho)=1 \\ (\mathbb{x},\mathbb{w})\notin R \end{array}\middle| \begin{array}{c} \tilde{\Pi}\leftarrow P \\ \mathbb{w}\leftarrow E(\tilde{\Pi}) \end{array}\right] = \Pr\left[\begin{array}{c} \rho\in A \\ V'^{\tilde{\Pi}}(\mathbb{x};\rho)=1 \\ (\mathbb{x},\mathbb{w})\notin R \end{array}\middle| \begin{array}{c} \tilde{\Pi}\leftarrow P \\ \mathbb{w}\leftarrow E(\tilde{\Pi}) \end{array}\right] + \Pr\left[\begin{array}{c} \rho\notin A \\ V^{\tilde{\Pi}}(\mathbb{x};\rho)=1 \\ (\mathbb{x},\mathbb{w})\notin R \end{array}\middle| \begin{array}{c} \tilde{\Pi}\leftarrow P \\ \mathbb{w}\leftarrow E(\tilde{\Pi}) \end{array}\right]$$

$$\leq \Pr\left[\begin{array}{c} V^{\tilde{\Pi}}(\mathbb{x};\rho)=1 \\ (\mathbb{x},\mathbb{w})\notin R \end{array}\middle| \begin{array}{c} \tilde{\Pi}\leftarrow P \\ \mathbb{w}\leftarrow E(\tilde{\Pi}) \end{array}\right] + \Pr\left[\rho\in A\right] \leq \kappa + \frac{k}{2^r}$$

Now we shall prove that (P', V') is not Γ-special sound after compilation with Kilian. Any accepting transcript set with challenges in A carries 0 information therefore it is not possible that some efficient algorithm can compute a valid witness given such a transcript set unless $R \in P$. □

Theorem 2.3. *Let $(\Gamma, \{0,1\}^r)$ be a monotone structure with at least one poly-bounded set in Γ. If there is a PCP with knowledge error κ that is Γ-special sound after compiling with Kilian then there is a PCP with knowledge error $\kappa + negl$ that is not Γ-special sound after compilation with Kilian.*

2.2 k-special soundness VS. Γ-special soundness

We saw how Kilians's protocol in general is not k or Γ-special soundness. Now we argue that Γ-special soundness is unlikely to offer any extra results.

Lemma 2.4. *Let (P, V) be a PCP with r bits of verifier randomness and knowledge error κ with extractor E. Define the following extractor E_{arg} for the interactive argument created by Kilian's protocol.*
E_{arg} :

1. *E_{arg} is given a set of k accepting transcripts $T = (\tau, (r_i, z_i)_{i\in[k]})$ for instance $\mathbb{x}$.*

2. *Create a proof string Π' by putting together all the locations revealed in T and fill the rest with $\perp$.*

3. *Run $\mathbb{w} \leftarrow E(\mathbb{x}, \Pi')$ and output witness $\mathbb{w}$.*

If Kilian's protocol is Γ-special sound and the corresponding extractor is E_{arg} and k is the size of the smallest set in Γ. E_{arg} can extract a valid witness given any set of k accepting transcripts.

Proof. Let T_r be the smallest set in Γ, T be a set of accepting transcripts with challenges in T_r, $\rho \in T_r$ and $\rho' \notin T_r$, it suffices to show that when $T'_r = T_r - \{\rho\} \cup \{\rho\}$ given an accepting transcript set T' for challenges in T'_r, E_{arg} can extract a valid witness. We create a new verifier V' as follows.
V' :

1. V' is given randomness ι.

2. If $\iota = \rho$, simulate $V(\rho')$.

3. If $\iota = \rho'$, simulate $V(\rho)$.

4. Otherwise, simulate $V(\iota)$.

It is easy to see that V and V' are functionally the same and any PCP extractor for V is also an extractor for V'. When (P, V') is compiled with Kilian, the resulting interactive argument is Γ-special sound with extractor E_{arg} (same as for (P, V) because they have the same PCP extractor), hence given a set of accepting transcripts T' (with respect to V' and $\mathbb{x}$) for challenges in T_r, E_{arg} will extract a valid witness. However notice that T' is also a set of accepting transcripts (with respect to V and $\mathbb{x}$) for challenges in T_r'. $\square$

It is a reasonable assumption that any extractor for arguments created by applying Kilian to PCPs should more or less look like E_{arg} as presented in Theorem 2.4, in particular extractors for (P, V) and (P, V') should be the same and therefore the lemma still holds. Notice that if Theorem 2.4 holds it means Γ-special soundness and k-special soundness are equivalent when k is the size of the smallest set in Γ.

Acknowledgments

Placeholder