

On Security Against Time Traveling Adversaries

Lúcás Críostóir Meier
lucas@cronokirby.com

September 2, 2022

Abstract

In this work, we investigate the notion of time travel, formally defining a model for adversaries equipped with a time machine, and the subsequent consequences on common cryptographic schemes.

1 Introduction

[Mau09]

2 Defining Abstract Games

In this section, we develop a framework to abstract over essentially all security games used to define the standalone security of cryptographic schemes.

We need such an abstraction in order to explore and compare different models of time travel. By having an abstract game, we can more easily define what it means to augment an adversary with the ability to travel through time, and we can more easily compare the differences between models of time travel across *all* games, rather than for just a particular cryptographic scheme.

2.1 State-Separable Proofs

But first, we need a basic notion of standalone security. For this, we lean on the framework of *state-separable proofs* [cite](#).

In this framework, you start with *packages*. A package P is defined by its code. This code describes how to initialize the state of the package, and what functions the package exports. These exported functions are denoted by the set $\text{out}(P)$. Each of these functions can accept input, produce output, and read and write to the internal state of the package. Packages may also have a set of imported functions, denoted by $\text{in}(P)$.

These imported functions are just “placeholders”, with no semantics. For them to have meaning, the package needs to be *linked* with another package. If A and

B are packages such that $\text{in}(A) \subseteq \text{out}(B)$, then we can define the composition package $A \circ B$. The exports are that of A , with $\text{out}(A \circ B) = \text{out}(A)$, and the imports that of B , with $\text{in}(A \circ B) = \text{in}(B)$. This package is implemented by merging the states of A and B , and replacing calls to the functions in $\text{in}(A)$ with the functionality defined in B .

A *game* G is a package with $\text{in}(G) = \emptyset$.

An *adversary* \mathcal{A} is a package with $\text{out}(\mathcal{A}) = \{\text{guess}\}$. The function `guess` takes no input, and returns a single bit \hat{b} . This bit represents the adversary's guess as to which of two games it's playing. Furthermore, if the function `guess` has a time complexity polynomial in a security parameter λ , we say that the adversary is *efficient*. Most commonly, we assume that all adversaries are efficient, unless we explicitly mark an adversary as *unbounded*.

By linking an adversary with a game, we get a package $\mathcal{A} \circ G$ with no imports, and a single export `guess`. This allows us to define the advantage of an adversary \mathcal{A} in distinguishing two games G_0, G_1 , via the formula:

$$\epsilon(\mathcal{A} \circ G_b) := |P[1 \leftarrow \text{guess}() \mid b = 0] - P[1 \leftarrow \text{guess}() \mid b = 1]|$$

Given we a pair of games G_0, G_1 , we say that they are:

- *equal*, denoted by $G_0 = G_1$, when $\epsilon(\mathcal{A} \circ G_b) = 0$ for any adversary, even unbounded.
- *indistinguishable*, denoted by $G_0 \approx G_1$, when $\epsilon(\mathcal{A} \circ G_b)$ is a negligible function of λ , for any *efficient* adversary (in λ).

The security of a cryptographic scheme is defined by a pair of games G_b . We say that the scheme is *secure* if $G_0 \approx G_1$.

For reductions, given game pairs G_b and H_b^1, \dots, H_b^N , and a function p , we write:

$$G_b \leq p(H_b^1, \dots, H_b^N)$$

If for any efficient adversary \mathcal{A} against G_b , there exists efficient adversaries $\mathcal{B}_1, \dots, \mathcal{B}_n$ such that:

$$\epsilon(\mathcal{A} \circ G_b) \leq p(\epsilon(\mathcal{B}_1 \circ H_b^1), \dots, \epsilon(\mathcal{B}_n \circ H_b^n))$$

2.2 Abstract Games

In the formalism of state-separable proofs, each game can have a different interface, and maintain a different kind of state. This is very useful, since it allows

us to capture various cryptographic schemes and notions of security. However, in order to easily model the impacts of time travel on various games, we would rather work with a *single* interface, capable of capturing the behavior of various games and their notions of security.

The key observation here is that the state of a pair of game is modified in only two places:

1. When the state is initialized.
2. When an exported function is called.

We can also collapse all of the exported functions into a single function, by including additional information in the input. For example, the input can include which sub-function is being called, along with the arguments to that sub-function.

The data we need to describe a game thus consist of a set of states Σ , an initialization function $\text{init} : () \xrightarrow{R} \Sigma$, as well as input and output types X and Y , along with a transition function $\text{next} : X \times \Sigma \rightarrow Y \times \Sigma$.

Together, these data define the following game:

$\mathcal{G}(\text{init}, \text{next})$

$s \leftarrow \text{init}()$

$\mathcal{O}(x) :$

$s, y \leftarrow \text{next}(s, x)$

return y

Game 1: $\mathcal{G}(\text{init}, \text{next})$

Intuitively, the game uses init to randomly initialize the state, and then each subsequent oracle call triggers some kind of randomized calculation which modifies the state, and produces an output.

We can also implicitly parameterize the types and functions with a bit b , allowing us to define the game pair $\mathcal{G}_b(\text{init}, \text{next})$, which is shorthand for $\mathcal{G}(\text{init}_b, \text{next}_b)$.

This abstract game is simple, but still expressive enough to capture any kind of game expressible in the state-separable formalism.

3 Models of Time Travel

In this section we investigate various models of time travel, and compare them with each other, showing that they form a hierarchy of increasingly strong capabilities.

The notion of time travel we explore is an intuitive one, inspired by science fiction. The adversary is equipped with a time machine, which allows them to travel forwards and backwards in time. However, the adversary must still be *efficient*. From their point of view, they only perform a number of operations polynomial in the security parameter λ , including time travel hops.

Some other models of time travel, like closed timelike curves, would allow, in essence, for computation with unbounded time (but bounded space) by an adversary. This is a much more powerful capability than we consider in this work, and unbounded computation breaks essentially all cryptography beyond information-theoretic schemes.

We also assume that time is *discrete*. Each interaction the adversary has with a game advances time forward by one step, and time hops can only be made between these discrete points in time. One potentially stronger capability would be to allow an adversary to “partially” undo the effects of an interaction, by rewinding an interaction before its completion. The reason we disallow this is because we assume the adversary has no other channels to learn about the state of the game beyond the information it gets from querying its exported functions. An adversary thus has no way of knowing where they need to time hop in order to partially undo an interaction, so we can make the simplifying assumption that all interactions are *atomic*, and time is discrete.

3.1 Rewinding Models

The first model of time travel we consider is that of *rewinding*, in which the adversary is allowed to travel backwards in time.

3.1.1 Single Rewinds

We start by giving the adversary the ability to travel backwards by exactly one time step.

We model this as a *transformation* between games. Given an abstract game \mathcal{G}_b , we define the game $\text{Rewind-1}(\mathcal{G}_b)$ as follows:

Rewind-1(\mathcal{G}_b)

$s_0 \leftarrow \text{init}()$

$i \leftarrow 0$

$\mathcal{O}(x) :$

$s_{i+1}, y \leftarrow \text{next}(s_i, x)$

return y

Rewind() :

assert $i > 0$

$i \leftarrow i - 1$

Game 2: Rewind-1(\mathcal{G}_b)

The interface is the same as that of \mathcal{G}_b , except that we now have an additional exported function: `Rewind`. Apart from this function, the behavior of the game is the same. Each interaction with \mathcal{O} advances the state. The difference is only in the internal implementation. Instead of a single state s , we now have a sequence of states s_0, s_1, \dots , as well as a position in this sequence, i .

The `Rewind` function is the additional capability here, and allows the adversary to move backwards by one step in time. This essentially models a very limited time machine, only allowing a small backwards movement in time.

Our first question is: does this limited model of time travel help the adversary? In other words, is an adversary with this capability more powerful than adversary without it? One way of capturing this notion of power would be to demonstrate a game \mathcal{E}_b which is *secure*, but where `Rewind-1`(\mathcal{E}_b) is broken. In fact, we can do this:

Claim 3.1. There exists a game \mathcal{E}_b and adversary \mathcal{A} such that \mathcal{E}_b is secure, yet $\epsilon(\mathcal{A} \circ \text{Rewind-1}(\mathcal{E}_b)) = 1$.

Consider the following game:

\mathcal{E}_b

$k_0, k_1 \xleftarrow{R} \{0, 1\}^\lambda$

queried $\leftarrow 0$

Query(σ) :

assert queried = 0

queried $\leftarrow 1$

return k_σ

Guess(\hat{k}_0, \hat{k}_1) :

assert $\hat{k}_0 = k_0 \wedge \hat{k}_1 = k_1$

return b

In this game, we have two random keys k_0, k_1 . The game lets the adversary choose to learn one of the keys, but not the other. If the adversary manages to guess both of the keys, then they'll be able to learn the value of b .

Now, because k_σ has λ bits, an adversary won't be able to randomly guess its value. This means that if the adversary only knows one of the keys, they won't be able to pass the assertion except with negligible probability. This means that \mathcal{E}_b is secure.

On the other hand, $\text{Rewind-1}(\mathcal{E}_b)$ is already broken. The following strategy will always succeed:

```

 $k_0 \leftarrow \text{Query}(0)$ 
 $\text{Rewind}()$ 
 $k_1 \leftarrow \text{Query}(1)$ 
 $b \leftarrow \text{Guess}(k_0, k_1)$ 
return  $b$ 

```

Even though the adversary prevents us from querying more than once, a single rewinding step is enough to undo our query, and thus learn the other key.

■

3.1.2 Multiple Rewinds

Next, we consider the ability to travel backwards by multiple steps at once. Like before, we model this with another transformation: Rewind-Many .

Rewind-Many(\mathcal{G}_b)	
$s_0 \leftarrow \text{init}()$	
$i \leftarrow 0$	
<u>$\mathcal{O}(x) :$</u>	<u>$\text{Rewind}(j) :$</u>
$s_{i+1}, y \leftarrow \text{next}(s_i, x)$	assert $i \geq j$
return y	$i \leftarrow i - j$

Game 3: $\text{Rewind-Many}(\mathcal{G}_b)$

The only difference with Rewind-1 is that now the adversary can specify a hop distance j , and move backwards by j steps, rather than by just a single step.

A natural question arises: is being able to jump backwards multiple steps at a time more powerful?

No.

Claim 3.2. Rewind-Many is as strong as Rewind-1. In particular, for any abstract game \mathcal{G}_b , we have $\text{Rewind-Many}(\mathcal{G}_b) \leq \text{Rewind-1}(\mathcal{G}_b)$.

The reduction works by emulating a large jump with many tiny jumps.

$$\text{Rewind-Many}(\mathcal{G}_b) = \boxed{\begin{array}{c} \Gamma \\ \hline \mathcal{O}(x) : \\ \text{return super}.\mathcal{O}(x) \end{array}} \begin{array}{c} \text{Rewind}(j) : \\ \text{assert } i \geq j \\ \text{super.Rewind() } j \text{ times} \end{array} \circ \text{Rewind-1}(\mathcal{G}_b)$$

The only subtlety is that we need to guarantee that this emulation is efficient, i.e. polynomial in λ . Because the adversary for \mathcal{A} against $\text{Rewind-Many}(\mathcal{G}_b)$ is efficient, we know that they make a number of queries to \mathcal{O} polynomial in λ . This means that the largest i they reach is also bounded, and thus so will the largest j they query. This means that the number of iterations we do in the emulation is also bounded by a polynomial in λ , so the reduction is efficient.

■

3.2 Forking Models

3.3 Summary

4 On Depth and Position Restrictions

5 Effects of Time Travel on Common Schemes

5.1 Stateless Schemes Remain Secure

5.2 On Encryption

5.3 On Signatures

6 Further Work

7 Conclusion

References

- [Mau09] Ueli Maurer. Unifying Zero-Knowledge Proofs of Knowledge. In *AFRICACRYPT 2009*, volume 5580 of *LNCS*, pages 272–286. Springer, Berlin, Heidelberg, 2009.