

EXHIBIT 12

Exhibit 12 – U.S. Patent No. 8,667,304 (“304 Patent”)

Claim 5	Roku Accused Instrumentalities
5[pre.1] A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause a client system in a second security domain to present content provided by a first conditional access server	The Roku Accused Instrumentalities include Roku devices compatible with HDCP, including, e.g., Roku 4K and 8K TVs. The screenshot shows a section of the Roku website titled 'Built by Roku' with the tagline 'The Roku experience inside and out.' Below this, there are three product cards. The first card is for the 'Plus Series 4K QLED' TV, featuring a large screen with a Roku interface and a 'Shop now' button. The second card is for the 'Select Series 4K' TV, also showing the Roku interface and a 'Shop now' button. The third card is for the 'Select Series HD' TV, showing the Roku interface and a 'Shop now' button. Each card includes a small Roku TV logo in the top left corner of the screen image. See, e.g., https://www.roku.com/products/roku-tv By way of example, the Accused Instrumentalities are configured to play HDCP-protected content (including, e.g., 4K Ultra HD and High Dynamic Range Content) via the HDMI interface of the Accused Instrumentalities, including e.g., streamed content from a streamed media device (e.g., a cable box, or other external streaming equipment).

Claim 5	Roku Accused Instrumentalities
	Tip: <i>If you receive your TV stations through a set top box from a cable or satellite TV provider, connect it to the TV using the best connection method available. From most to least desirable:</i> • HDMI® input – Digital HD and SD video • AV input – analog SD video • Antenna input – analog SD video using NTSC See, e.g., https://image.roku.com/c3VwcG9ydC1B/Roku-TV-User-Guide-10-0-en-US-.pdf To the extent the preamble is limiting, the Accused Instrumentalities incorporate a non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause a client system in a second security domain to present content provided by a first conditional access server. For example, the Roku Accused Instrumentalities are client systems in a second security domain (e.g., a security domain associated with HDCP). The Roku Accused Instrumentalities employ memory, such as RAM memory (examples shown in the red box in the below figure), to store executable program instructions (e.g., the Roku OS operating system and/or other firmware for the operation of the Accused Instrumentalities). Each Roku Accused Instrumentality includes a data processing system (e.g., a processor such as those shown in the blue box in the below figure). Executing the computer program instructions by the data processing system causes content in a second security domain (e.g., HDCP security domain, shown in the light green box in the below figure) to be presented (e.g., played or provided for playing) by the Roku Accused Instrumentalities. The content originally is provided by a first conditional access server (e.g., a streaming content server).

Claim 5**Roku Accused Instrumentalities**

Device Name	Code Name	roDeviceInfo.GetModel()	CPU	Accelerated Graphics API	RAM	Max UI Resolution	Max Playback Resolution	HDR Support
Roku TV	Roxton	K000X	ARM Cortex A35	OpenGL ES 2.0	512 MB	720p	1080p/60fps	No
Roku TV (Brazil)	El Paso	8000X	ARM	OpenGL ES 2.0	512 MB	720p	1080p	No
Roku Smart Soundbar	Fruitland	9100X	ARM Cortex A53	OpenGL ES 2.0	1 GB	1080p	4K60fps, HDR	HDR10
Roku Streambar	Chico	9102X	MStar C2	OpenGL ES 2.0	1 GB	1080p/60fps	4K60fps, HDR	HDR10 and HLG
2K Roku TV	Miami	H000X	ARM quad core 1 GHz	OpenGL ES 2.0	512MB	720p	1080p/60fps	No
4K Roku TV	Reno	A000X	ARM quad core 1 GHz	OpenGL ES 2.0	1.5 GB	1920X1080	3840x2160	HDR10, Dolby Vision, and HLG supported, varies by model
4K Roku TV	Malone	C000X	ARM quad core 1 GHz	OpenGL ES 2.0	1 GB	1920X1080	3840x2160	HDR10, Dolby Vision, and HLG supported, varies by model
4K Roku TV	Athens	G000X	ARM quad core 1 GHz	OpenGL ES 2.0	1 GB	1920X1080	3840x2160	HDR10, Dolby Vision, and HLG supported, varies by model
4K Roku TV (EU)	Camden	C000GB	ARM quad core 1 GHz	OpenGL ES 2.0	1 GB	1920X1080	3840x2160	HDR10, Dolby Vision, and HLG supported, varies by model
8K Roku TV	Bandera	E000X	ARM quad core 1 GHz	OpenGL ES 2.0	1.5 GB	1920X1080	7.680x4.320	HDR10, Dolby Vision, and HLG supported, varies by model

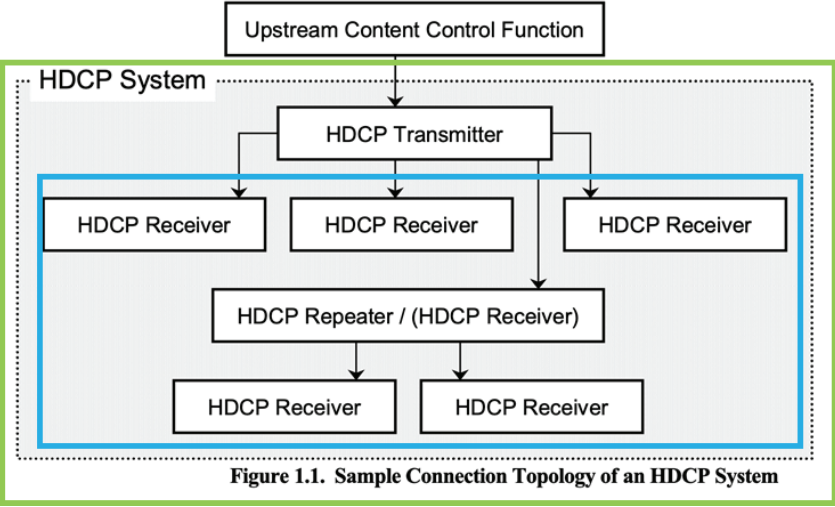
See, e.g., <https://developer.roku.com/docs/specs/hardware.md>

What is HDCP 2.2?

The latest copy protection technology is called HDCP (High-bandwidth Digital Content Protection) and is used on HDMI connections for digital devices like Blu-ray™ players, cable boxes and Roku streaming devices. HDCP is the copy and content protection standard used by the movie and TV industry. Copy protection/content protection has been around for a long time, and in its early stages was what prevented you from copying commercial VHS tapes. **HDCP 2.2** is specifically designed for [4K Ultra HD](#) content, as well as movies and TV shows available with [High Dynamic Range](#).

See, e.g., <https://support.roku.com/article/230317588>

Claim 5	Roku Accused Instrumentalities
	Why is HDCP 2.2 important to playing 4K Ultra HD or HDR content? To successfully stream 4K Ultra HD (4K) or High Dynamic Range (HDR) content, all devices connected via HDMI[®] to your compatible Roku[®] streaming player must support HDCP 2.2. This includes your TV, an audio/video receiver (AVR), and any other devices connected in between. If even one device does not support HDCP 2.2, then the 4K or HDR movie or TV show can only be viewed in a lower resolution, such as 720p or 1080p. <i>See, e.g.,</i> https://support.roku.com/article/230317588 1. Connecting directly to a compatible 4K TV  a. Connect the opposite end of the HDMI cable that is attached to your Roku player, or connect your Streaming Stick to an available HDMI 2.0 input on your TV that supports HDCP 2.2. <i>See, e.g.,</i> https://support.roku.com/article/211194548

Claim 5	Roku Accused Instrumentalities
	 Figure 1.1. Sample Connection Topology of an HDCP System <i>See, e.g.,</i> HDCP on HDMI Specification, Rev. 2.2
5[pre.2] wherein the first conditional access server has authenticated a client device of the first conditional access server through a first authentication process using a first root of trust for a first security domain and	The Accused Instrumentalities are configured to be connected to streaming media devices (e.g., Roku streaming media devices, cable boxes, or other external streaming equipment) via an HDMI interface for streaming 4K Ultra HD and High Dynamic Range Content. The Accused Instrumentalities are configured to receive high-bandwidth data. Data received by the streaming device for use in the Accused Instrumentalities is protected with DRM functionality such as PlayReady and/or Widevine:

Claim 5**Roku Accused Instrumentalities****Digital rights management (DRM) control attributes**

Available since Roku OS 8.1

Digital rights management (DRM) content meta-data control attributes are available in the Roku OS through the `drmParams` parameter of type `roAssociativeArray`. The table below enum all usable attributes of `drmParams`.

Note: Not all attributes are required, and may not have the same semantic meaning when applied to different DRM systems.

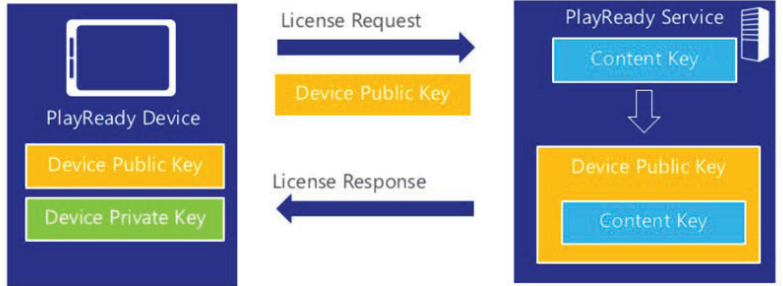
Attribute	DRM System	Type	Value	Example
appData	Playready, Widevine, Verimatrix; Optional	String	Special meaning per DRM system. If supplied, expected to be a base64 encoded string.	"5GF2Z5B0byBkZWFiHdpdGggQmFzZTY0IGZ..."
encodingKey	Playready; Optional	String	This field is deprecated; use the <code>licenseServerURL</code> field. Specifies the PlayReady license acquisition data, in format depending on the <code>encodingType</code> attribute value specified: when <code>encodingType</code>="PlayReadyLicenseAcquisitionUrl", the <code>EncodingKey</code> attribute contains the PlayReady license acquisition URL	"http://serverName/"
encodingType	Playready; Optional	String	This field is deprecated; use the <code>licenseServerURL</code> field. Specifies the encoding scheme for PlayReady DRM, by setting to one of the following values: "PlayReadyLicenseAcquisitionUrl" "PlayReadyLicenseAcquisitionAndChallenge" Note, this is the same value that used to be specified directly in Content Metadata structure	"PlayReadyLicenseAcquisitionAndChallenge"
keySystem	Required for all	String	"playready" or "widevine". This value is case-insensitive. The default is an empty string.	"widevine"

See, e.g., <https://developer.roku.com/en-gb/docs/developer-program/getting-started/architecture/content-metadata.md>

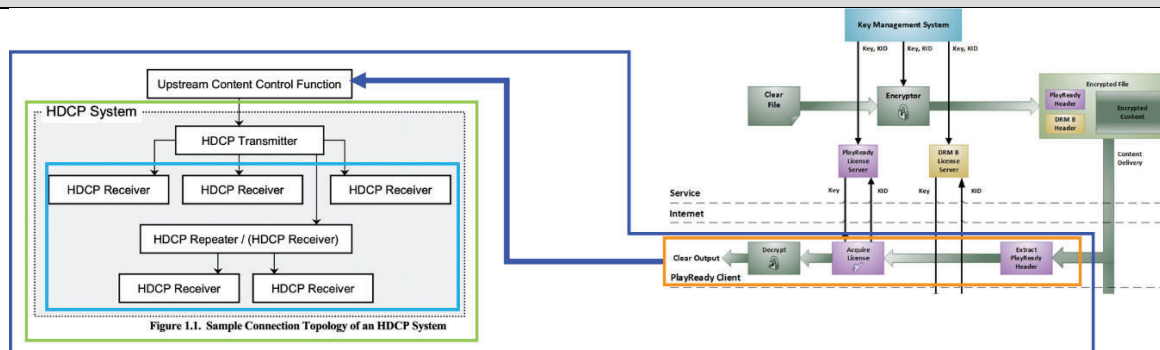
	PlayReady	AES-128	Widevine
HLS			Y
Smooth	Y		
DASH	Y		Y

See, e.g., <https://developer.roku.com/en-gb/docs/specs/media/content-protection.md>

To the extent the preamble is limiting, the first conditional access server has authenticated a client device of the first conditional access server through a first authentication process using

Claim 5	Roku Accused Instrumentalities
	a first root of trust for a first security domain. For example, the first conditional access server (e.g., the streaming content server) authenticated a streaming media device using a PlayReady root of trust in a first security domain (e.g., PlayReady DRM, in the example shown below). As another example, the first conditional access server authenticates a streaming media device using a Widevine root of trust in the Widevine DRM security domain. Client Authentication In the context of content protection, client authentication may occur at two levels, the client device and the user. PlayReady handles device authentication automatically through its use of <u>device keys when issuing licenses to PlayReady clients</u>, as illustrated in the following diagram.  Figure 4 – Role of Device Keys in the Licensing Process See, e.g., https://download.microsoft.com/download/B/D/4/BD42A75B-5B3E-49C0-B70D-DD49FA9592F9/DevelopingMicrosoftPlayReadyClients_March2015.pdf, p12 <u>Each PlayReady client device has a unique public-private key pair. When a client sends a license request to a license service, it includes its device public key. The license service uses that public key to verify that the client device is a valid PlayReady client before it issues the license. If the device is a valid PlayReady client, the license service uses the device's public key to encrypt the content key for the media file and then sends the resulting license to the client. The client must then use its device private key to decrypt and play back the content. This authentication model ensures that the issued license is valid and usable only on that device (in the case of the device binding).</u>

Claim 5	Roku Accused Instrumentalities
	<i>See, e.g.,</i> https://download.microsoft.com/download/B/D/4/BD42A75B-5B3E-49C0-B70D-DD49FA9592F9/DevelopingMicrosoftPlayReadyClients_March2015.pdf, p12 PlayReady Certificate Authority Microsoft owns the PlayReady Certificate Authority (PlayReady CA) including the PlayReady top level CA certificates, which gives Microsoft the authority to deliver PlayReady certificates to its customers, and revoke them whenever it is required to keep the ecosystem functional and secure. <i>See, e.g.,</i> https://learn.microsoft.com/en-us/playready/overview/certificates
5[pre.3] wherein a second conditional access server is configured to substitute the first security domain with the second security domain for client devices under a second root of trust, the method comprising:	To the extent the preamble is limiting, a second conditional access server is configured to substitute the first security domain with the second security domain for client devices under a second root of trust. For example, a second conditional access server (e.g., the streaming media device that serves content to the Accused Functionality) decrypts the content in the first security domain (e.g., the PlayReady DRM-protected content or Widevine DRM-protected content, shown in the orange box in the below figure) and re-encrypts the content in the second security domain (e.g., using HDCP encryption, shown in the light green box in the below figure) for client devices under a second root of trust (e.g., that support HDCP as shown in the light blue box in the below figure).

Claim 5**Roku Accused Instrumentalities**

See, e.g., HDCP on HDMI Specification, Rev. 2.2; <https://learn.microsoft.com/en-us/playready/overview/playready-and-other-protection-technologies>

HDCP employs an established authentication process and root of trust for HDCP client devices.

2 Authentication Protocol

2.1 Overview

The HDCP authentication protocol is an exchange between an HDCP Transmitter and an HDCP Receiver that affirms to the HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. It is comprised of the following stages

- Authentication and Key Exchange (AKE) – The HDCP Receiver's public key certificate is verified by the HDCP Transmitter. A Master Key k_m is exchanged.
- Locality Check – The HDCP Transmitter enforces locality on the content by requiring that the Round Trip Time (RTT) between a pair of messages is not more than 20 ms.
- Session Key Exchange (SKE) – The HDCP Transmitter exchanges Session Key k_s with the HDCP Receiver.

Claim 5	Roku Accused Instrumentalities																								
	The HDCP Transmitter contains the 3072-bit RSA public key of DCP LLC denoted by $kpub_{dcp}$. The HDCP Receiver is issued 1024-bit RSA public and private keys. The public key is stored in a Public Key Certificate issued by DCP LLC, denoted by $cert_{rx}$. Table 2.1 gives the fields contained in the certificate. All values are stored in big-endian format. <table><tr><th>Name</th><th>Size (bits)</th><th>Bit position</th><th>Function</th></tr><tr><td>Receiver ID</td><td>40</td><td>4175:4136</td><td>Unique receiver identifier. It has the same format as an HDCP 1.x KSV i.e. it contains 20 ones and 20 zeroes</td></tr><tr><td>Receiver Public Key</td><td>1048</td><td>4135:3088</td><td>Unique RSA public key of HDCP Receiver denoted by $kpub_{rx}$. The first 1024 bits is the big-endian representation of the modulus n and the trailing 24 bits is the big-endian representation of the public exponent e</td></tr><tr><td>Reserved2</td><td>4</td><td>3087:3084</td><td>Reserved for future definition. Must be 0x0 or 0x1.</td></tr><tr><td>Reserved1</td><td>12</td><td>3083:3072</td><td>Reserved for future definition. Must be 0x000</td></tr><tr><td>DCP LLC Signature</td><td>3072</td><td>3071:0</td><td>A cryptographic signature calculated over all preceding fields of the certificate. RSASSA-PKCS1-v1_5 is the signature scheme used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function</td></tr></table> Table 2.1. Public Key Certificate of HDCP Receiver See, e.g., HDCP on HDMI Specification, Rev. 2.2, pp. 11-12	Name	Size (bits)	Bit position	Function	Receiver ID	40	4175:4136	Unique receiver identifier. It has the same format as an HDCP 1.x KSV i.e. it contains 20 ones and 20 zeroes	Receiver Public Key	1048	4135:3088	Unique RSA public key of HDCP Receiver denoted by $kpub_{rx}$. The first 1024 bits is the big-endian representation of the modulus n and the trailing 24 bits is the big-endian representation of the public exponent e	Reserved2	4	3087:3084	Reserved for future definition. Must be 0x0 or 0x1.	Reserved1	12	3083:3072	Reserved for future definition. Must be 0x000	DCP LLC Signature	3072	3071:0	A cryptographic signature calculated over all preceding fields of the certificate. RSASSA-PKCS1-v1_5 is the signature scheme used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function
Name	Size (bits)	Bit position	Function																						
Receiver ID	40	4175:4136	Unique receiver identifier. It has the same format as an HDCP 1.x KSV i.e. it contains 20 ones and 20 zeroes																						
Receiver Public Key	1048	4135:3088	Unique RSA public key of HDCP Receiver denoted by $kpub_{rx}$. The first 1024 bits is the big-endian representation of the modulus n and the trailing 24 bits is the big-endian representation of the public exponent e																						
Reserved2	4	3087:3084	Reserved for future definition. Must be 0x0 or 0x1.																						
Reserved1	12	3083:3072	Reserved for future definition. Must be 0x000																						
DCP LLC Signature	3072	3071:0	A cryptographic signature calculated over all preceding fields of the certificate. RSASSA-PKCS1-v1_5 is the signature scheme used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function																						
5[a] receiving, at a second conditional access client of the second conditional access server, an authentication through a second authentication process which is independent of the first authentication process and	The Accused Instrumentalities receive an authentication through a second authentication process which is independent of the first authentication process. For example, the Accused Instrumentalities receive an authentication using the HDCP authentication process (shown in the blue boxes in the below figures), which is independent of the first authentication process (e.g., DRM).																								

Claim 5	Roku Accused Instrumentalities																								
	2 Authentication Protocol 2.1 Overview The HDCP authentication protocol is an exchange between an HDCP Transmitter and an HDCP Receiver that affirms to the HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. It is comprised of the following stages • Authentication and Key Exchange (AKE) – The HDCP Receiver’s public key certificate is verified by the HDCP Transmitter. A Master Key k_m is exchanged. • Locality Check – The HDCP Transmitter enforces locality on the content by requiring that the Round Trip Time (RTT) between a pair of messages is not more than 20 ms. • Session Key Exchange (SKE) – The HDCP Transmitter exchanges Session Key k_s with the HDCP Receiver. The HDCP Transmitter contains the 3072-bit RSA public key of DCP LLC denoted by $k_{pub_{dcp}}$. The HDCP Receiver is issued 1024-bit RSA public and private keys. The public key is stored in a Public Key Certificate issued by DCP LLC, denoted by $cert_{rx}$. Table 2.1 gives the fields contained in the certificate. All values are stored in big-endian format. <table><thead><tr><th>Name</th><th>Size (bits)</th><th>Bit position</th><th>Function</th></tr></thead><tbody><tr><td>Receiver ID</td><td>40</td><td>4175:4136</td><td>Unique receiver identifier. It has the same format as an HDCP 1.x KSV i.e. it contains 20 ones and 20 zeroes</td></tr><tr><td>Receiver Public Key</td><td>1048</td><td>4135:3088</td><td>Unique RSA public key of HDCP Receiver denoted by $k_{pub_{rx}}$. The first 1024 bits is the big-endian representation of the modulus n and the trailing 24 bits is the big-endian representation of the public exponent e</td></tr><tr><td>Reserved2</td><td>4</td><td>3087:3084</td><td>Reserved for future definition. Must be 0x0 or 0x1.</td></tr><tr><td>Reserved1</td><td>12</td><td>3083:3072</td><td>Reserved for future definition. Must be 0x000</td></tr><tr><td>DCP LLC Signature</td><td>3072</td><td>3071:0</td><td>A cryptographic signature calculated over all preceding fields of the certificate. RSASSA-PKCS1-v1_5 is the signature scheme used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function</td></tr></tbody></table> Table 2.1. Public Key Certificate of HDCP Receiver See, e.g., HDCP on HDMI Specification, Rev. 2.2, pp. 11-12	Name	Size (bits)	Bit position	Function	Receiver ID	40	4175:4136	Unique receiver identifier. It has the same format as an HDCP 1.x KSV i.e. it contains 20 ones and 20 zeroes	Receiver Public Key	1048	4135:3088	Unique RSA public key of HDCP Receiver denoted by $k_{pub_{rx}}$. The first 1024 bits is the big-endian representation of the modulus n and the trailing 24 bits is the big-endian representation of the public exponent e	Reserved2	4	3087:3084	Reserved for future definition. Must be 0x0 or 0x1.	Reserved1	12	3083:3072	Reserved for future definition. Must be 0x000	DCP LLC Signature	3072	3071:0	A cryptographic signature calculated over all preceding fields of the certificate. RSASSA-PKCS1-v1_5 is the signature scheme used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function
Name	Size (bits)	Bit position	Function																						
Receiver ID	40	4175:4136	Unique receiver identifier. It has the same format as an HDCP 1.x KSV i.e. it contains 20 ones and 20 zeroes																						
Receiver Public Key	1048	4135:3088	Unique RSA public key of HDCP Receiver denoted by $k_{pub_{rx}}$. The first 1024 bits is the big-endian representation of the modulus n and the trailing 24 bits is the big-endian representation of the public exponent e																						
Reserved2	4	3087:3084	Reserved for future definition. Must be 0x0 or 0x1.																						
Reserved1	12	3083:3072	Reserved for future definition. Must be 0x000																						
DCP LLC Signature	3072	3071:0	A cryptographic signature calculated over all preceding fields of the certificate. RSASSA-PKCS1-v1_5 is the signature scheme used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function																						
5[b] wherein the second authentication process uses the second root of trust for the second	The second authentication process uses the second root of trust for the second security domain which is independent of and different than the first root of trust.																								

Claim 5	Roku Accused Instrumentalities
security domain which is independent of and different than the first root of trust; and	For example, the HDCP authentication process (shown in the blue boxes in the below figures) uses a different root of trust than the PlayReady root of trust (or the Widevine root of trust) (shown in the yellow boxes and highlighting in the below figures). <u>Each PlayReady client device has a unique public-private key pair. When a client sends a license request to a license service, it includes its device public key. The license service uses that public key to verify that the client device is a valid PlayReady client before it issues the license. If the device is a valid PlayReady client, the license service uses the device's public key to encrypt the content key for the media file and then sends the resulting license to the client. The client must then use its device private key to decrypt and play back the content. This authentication model ensures that the issued license is valid and usable only on that device (in the case of the device binding).</u> <i>See, e.g.,</i> https://download.microsoft.com/download/B/D/4/BD42A75B-5B3E-49C0-B70D-DD49FA9592F9/DevelopingMicrosoftPlayReadyClients_March2015.pdf, p12 PlayReady Certificate Authority Microsoft owns the PlayReady Certificate Authority (PlayReady CA) including the PlayReady top level CA certificates, which gives Microsoft the authority to deliver PlayReady certificates to its customers, and revoke them whenever it is required to keep the ecosystem functional and secure. <i>See, e.g.,</i> https://learn.microsoft.com/en-us/playready/overview/certificates

Claim 5	Roku Accused Instrumentalities																								
	2 Authentication Protocol 2.1 Overview The HDCP authentication protocol is an exchange between an HDCP Transmitter and an HDCP Receiver that affirms to the HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. It is comprised of the following stages • Authentication and Key Exchange (AKE) – The HDCP Receiver’s public key certificate is verified by the HDCP Transmitter. A Master Key k_m is exchanged. • Locality Check – The HDCP Transmitter enforces locality on the content by requiring that the Round Trip Time (RTT) between a pair of messages is not more than 20 ms. • Session Key Exchange (SKE) – The HDCP Transmitter exchanges Session Key k_s with the HDCP Receiver. The HDCP Transmitter contains the 3072-bit RSA public key of DCP LLC denoted by $k_{pub_{dcp}}$. The HDCP Receiver is issued 1024-bit RSA public and private keys. The public key is stored in a Public Key Certificate issued by DCP LLC, denoted by $cert_{rx}$. Table 2.1 gives the fields contained in the certificate. All values are stored in big-endian format. <table><thead><tr><th>Name</th><th>Size (bits)</th><th>Bit position</th><th>Function</th></tr></thead><tbody><tr><td>Receiver ID</td><td>40</td><td>4175:4136</td><td>Unique receiver identifier. It has the same format as an HDCP 1.x KSV i.e. it contains 20 ones and 20 zeroes</td></tr><tr><td>Receiver Public Key</td><td>1048</td><td>4135:3088</td><td>Unique RSA public key of HDCP Receiver denoted by $k_{pub_{rx}}$. The first 1024 bits is the big-endian representation of the modulus n and the trailing 24 bits is the big-endian representation of the public exponent e</td></tr><tr><td>Reserved2</td><td>4</td><td>3087:3084</td><td>Reserved for future definition. Must be 0x0 or 0x1.</td></tr><tr><td>Reserved1</td><td>12</td><td>3083:3072</td><td>Reserved for future definition. Must be 0x000</td></tr><tr><td>DCP LLC Signature</td><td>3072</td><td>3071:0</td><td>A cryptographic signature calculated over all preceding fields of the certificate. RSASSA-PKCS1-v1_5 is the signature scheme used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function</td></tr></tbody></table> Table 2.1. Public Key Certificate of HDCP Receiver See, e.g., HDCP on HDMI Specification, Rev. 2.2, pp. 11-12	Name	Size (bits)	Bit position	Function	Receiver ID	40	4175:4136	Unique receiver identifier. It has the same format as an HDCP 1.x KSV i.e. it contains 20 ones and 20 zeroes	Receiver Public Key	1048	4135:3088	Unique RSA public key of HDCP Receiver denoted by $k_{pub_{rx}}$. The first 1024 bits is the big-endian representation of the modulus n and the trailing 24 bits is the big-endian representation of the public exponent e	Reserved2	4	3087:3084	Reserved for future definition. Must be 0x0 or 0x1.	Reserved1	12	3083:3072	Reserved for future definition. Must be 0x000	DCP LLC Signature	3072	3071:0	A cryptographic signature calculated over all preceding fields of the certificate. RSASSA-PKCS1-v1_5 is the signature scheme used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function
Name	Size (bits)	Bit position	Function																						
Receiver ID	40	4175:4136	Unique receiver identifier. It has the same format as an HDCP 1.x KSV i.e. it contains 20 ones and 20 zeroes																						
Receiver Public Key	1048	4135:3088	Unique RSA public key of HDCP Receiver denoted by $k_{pub_{rx}}$. The first 1024 bits is the big-endian representation of the modulus n and the trailing 24 bits is the big-endian representation of the public exponent e																						
Reserved2	4	3087:3084	Reserved for future definition. Must be 0x0 or 0x1.																						
Reserved1	12	3083:3072	Reserved for future definition. Must be 0x000																						
DCP LLC Signature	3072	3071:0	A cryptographic signature calculated over all preceding fields of the certificate. RSASSA-PKCS1-v1_5 is the signature scheme used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function																						
5[c] receiving, at the second conditional access client, content that is in an access controlled	The Accused Instrumentalities receive content that is in an access controlled format specified by the second conditional access server in the second security domain, the second conditional access client being in the second security domain.																								

Claim 5	Roku Accused Instrumentalities
format specified by the second conditional access server in the second security domain, the second conditional access client being in the second security domain.	For example, the Accused Instrumentalities receive (e.g., using an HDCP Receiver) content in an access controlled format (e.g., HDCP encrypted content) in a second security domain (e.g., as shown in the pink box below), such as a HDCP encrypted security domain. For the purpose of this specification, it is assumed that the Audiovisual content is transmitted over a HDMI based wired display link. In an HDCP System, two or more HDCP Devices are interconnected through an HDCP-protected Interface. The Audiovisual Content flows from the Upstream Content Control Function into the HDCP System at the most upstream HDCP Transmitter. From there <u>the Audiovisual Content encrypted by the HDCP System, referred to as HDCP Content,</u> flows through a tree-shaped topology of <u>HDCP Receivers over HDCP-protected Interfaces.</u> This specification describes a content protection mechanism for: (1) authentication of HDCP Receivers to their immediate upstream connection (i.e., an HDCP Transmitter), (2) revocation of HDCP Receivers that are determined by the Digital Content Protection, LLC, to be invalid, and (3) <u>HDCP Encryption of Audiovisual Content over the HDCP-protected Interfaces between HDCP Transmitters and their downstream HDCP Receivers.</u> HDCP Receivers may render the HDCP Content in audio and visual form for human consumption. HDCP Receivers may be HDCP Repeaters that serve as downstream HDCP Transmitters emitting the HDCP Content further downstream to one or more additional HDCP Receivers. <i>See, e.g.,</i> HDCP on HDMI Specification, Rev. 2.2

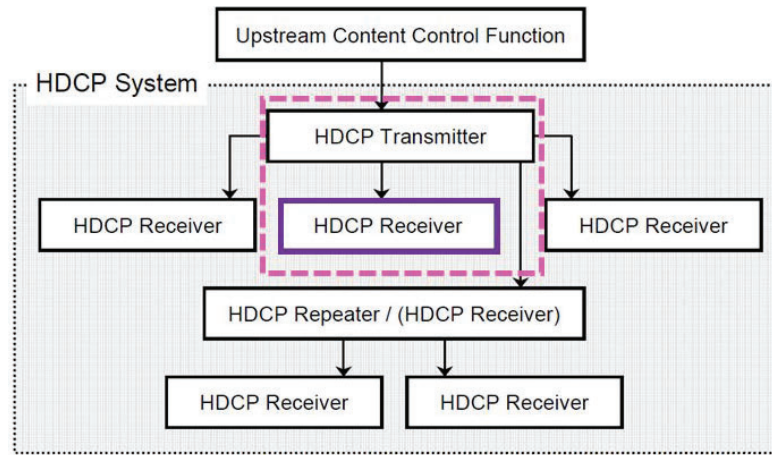
Claim 5**Roku Accused Instrumentalities**

Figure 1.1. Sample Connection Topology of an HDCP System

See, e.g., HDCP on HDMI Specification, Rev. 2.2

3 HDCP Encryption**3.1 Data Encryption**

HDCP Encryption is applied at the input to the T.M.D.S. Encoder and decryption is applied at the output of the T.M.D.S. Decoder (Figure 3-1). HDCP Encryption consists of a bit-wise exclusive-or (XOR) of the HDCP Content with a pseudo-random data stream produced by the HDCP Cipher.

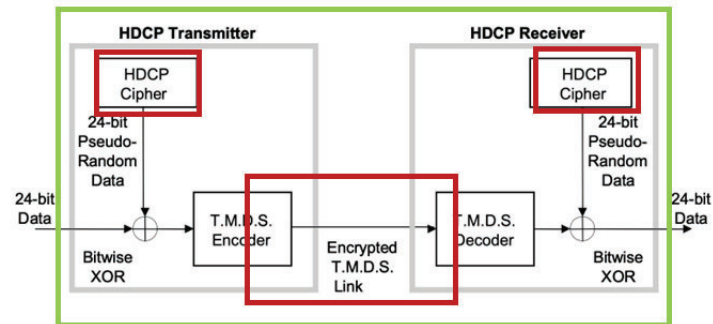


Figure 3-1. HDCP Encryption and Decryption

Claim 5	Roku Accused Instrumentalities
	<i>See, e.g.</i>, HDCP on HDMI Specification, Rev. 2.2 The access controlled format is specified by the second conditional access server. For example, streaming media devices derive HDCP control information from PlayReady (or Widevine) licensing information, including for 4K and UHD content. Each license contains the following information: • The content encryption key. • The rights of the license. • The right restrictions and right modifiers, also known as the conditions of the license. Before a client can decrypt the content associated with a license, it must retrieve the policy from the license. The content protection information within the license is encrypted using a client's public key or a client's domain's public key encryption information. The license is considered "bound" to the client or domain that has the private key for decrypting the content protection information. Clients acquire licenses either directly from License Servers or through a Proxy Server. <i>See, e.g.</i>, https://learn.microsoft.com/en-us/playready/overview/license-acquisition Rights Restrictions and other Policies The PlayReady Compliance Rules contain a full list of right modifiers (extensions and restrictions) that may apply to the license. Each of these modifiers has multiple properties: • Action—specifies the action of the policy (for example, engage HDCP encryption on the HDMI output). • Optional—specifies if the client must engage the action or must try to engage the action (for example, Output Control for Uncompressed Digital Video Content 250, see CR 3.6.5). <i>See, e.g.</i>, https://learn.microsoft.com/en-us/playready/overview/license-and-policies

Claim 5	Roku Accused Instrumentalities																																	
	The Accused Instrumentalities receive content over the HDMI interface as HDCP encrypted content in accordance with engaging the HDCP requirements of the PlayReady (or Widevine) HDCP enforcement requirements as specified by the streaming media device during engagement of HDCP over HDMI. <table><tr><th rowspan="2">OPL</th><th>Compressed Digital Video</th><th colspan="2">Uncompressed Digital Video</th><th>Analog TV</th></tr><tr><th>Any</th><th colspan="2">HDMI, DVI, DisplayPort, MHL</th><th>Component, Composite</th></tr><tr><td>0-100</td><td rowspan="4">Block</td><td colspan="2" rowspan="3">Passes content</td><td>Passes content</td></tr><tr><td>101-150</td><td>Passes content when CGMS-A CopyNever is engaged or if CGMS-A can't be engaged.</td></tr><tr><td>151-200</td><td>Passes content when CGMS-A CopyNever is engaged.</td></tr><tr><td>201-250</td><td colspan="2">Attempts to engage HDCP, but passes content regardless of result.</td><td rowspan="3">Does NOT pass content</td></tr><tr><td>251-270</td><td colspan="2"> SWDRM: Attempts to engage HDCP. If HDCP fails to engage, the PC will constrain the effective resolution to 520,000 pixels per frame and pass the content. HWDRM: Passes content with HDCP. If HDCP fails to engage, playback to HDMI/DVI ports is blocked. </td></tr><tr><td>271-300</td><td colspan="2">When HDCP type restriction is NOT defined: Passes content with HDCP. If HDCP fails to engage, playback to HDMI/DVI ports is blocked. When HDCP type restriction IS defined: Passes content with HDCP 2.2 and content stream type set to 1. If HDCP fails to engage or content stream type can't be set to 1, playback to HDMI/DVI ports is blocked.</td></tr><tr><td>> 300</td><td></td><td colspan="2">Does NOT pass content</td><td></td></tr></table> See, e.g., https://learn.microsoft.com/en-us/playready/overview/output-protection-levels	OPL	Compressed Digital Video	Uncompressed Digital Video		Analog TV	Any	HDMI, DVI, DisplayPort, MHL		Component, Composite	0-100	Block	Passes content		Passes content	101-150	Passes content when CGMS-A CopyNever is engaged or if CGMS-A can't be engaged.	151-200	Passes content when CGMS-A CopyNever is engaged.	201-250	Attempts to engage HDCP, but passes content regardless of result.		Does NOT pass content	251-270	SWDRM: Attempts to engage HDCP. If HDCP fails to engage, the PC will constrain the effective resolution to 520,000 pixels per frame and pass the content. HWDRM: Passes content with HDCP. If HDCP fails to engage, playback to HDMI/DVI ports is blocked.		271-300	When HDCP type restriction is NOT defined: Passes content with HDCP. If HDCP fails to engage, playback to HDMI/DVI ports is blocked. When HDCP type restriction IS defined: Passes content with HDCP 2.2 and content stream type set to 1. If HDCP fails to engage or content stream type can't be set to 1, playback to HDMI/DVI ports is blocked.		> 300		Does NOT pass content		
OPL	Compressed Digital Video		Uncompressed Digital Video		Analog TV																													
	Any	HDMI, DVI, DisplayPort, MHL		Component, Composite																														
0-100	Block	Passes content		Passes content																														
101-150				Passes content when CGMS-A CopyNever is engaged or if CGMS-A can't be engaged.																														
151-200				Passes content when CGMS-A CopyNever is engaged.																														
201-250		Attempts to engage HDCP, but passes content regardless of result.		Does NOT pass content																														
251-270	SWDRM: Attempts to engage HDCP. If HDCP fails to engage, the PC will constrain the effective resolution to 520,000 pixels per frame and pass the content. HWDRM: Passes content with HDCP. If HDCP fails to engage, playback to HDMI/DVI ports is blocked.																																	
271-300	When HDCP type restriction is NOT defined: Passes content with HDCP. If HDCP fails to engage, playback to HDMI/DVI ports is blocked. When HDCP type restriction IS defined: Passes content with HDCP 2.2 and content stream type set to 1. If HDCP fails to engage or content stream type can't be set to 1, playback to HDMI/DVI ports is blocked.																																	
> 300		Does NOT pass content																																

Claim 5	Roku Accused Instrumentalities					
		<table><tr><td>content_key_specs. required_output_protection. hdcv</td><td>string - one of: HDCP_NONE, HDCP_V1, HDCP_V2</td><td>Indicates whether HDCP is required. Default = HDCP_NONE. Note: These must be capitalized, lowercase will result in a malformed request. See Appendix.</td></tr></table>	content_key_specs. required_output_protection. hdcv	string - one of: HDCP_NONE, HDCP_V1, HDCP_V2	Indicates whether HDCP is required. Default = HDCP_NONE. Note: These must be capitalized, lowercase will result in a malformed request. See Appendix .	
content_key_specs. required_output_protection. hdcv	string - one of: HDCP_NONE, HDCP_V1, HDCP_V2	Indicates whether HDCP is required. Default = HDCP_NONE. Note: These must be capitalized, lowercase will result in a malformed request. See Appendix .				
	See, e.g., Widevine DRM Proxy Integration					