# Efficient Stream Authentication in Secure Wireless Multimedia Space Networks: The Source-Authentication-Protocol Optimality

Chunqiu Wang, Wei Wang*, Runan Yao
Department of Electrical Engineering and Computer Science
South Dakota State University, Brookings, SD 57007, USA
Email: {chunqiu.wang, wei.wang, runan.yao}@sdstate.edu

***Abstract*—Resource constrained secure deep space Inter-Planetary Multimedia Networks (IPMNs) gathering various planetary sensor information have high requirements for energy-efficient transmission, error-resilient multimedia coding and robust content authentication. However, the joint exploration of Intra-Inter video coding versatility in signal processing domain, Signature-Hash diversity in information security domain and Forward Channel Correction (FEC) channel coding application in network protocol domain has largely been ignored in literature. In this paper, we propose a new Source-Authentication-Protocol (SAP) framework to provide multimedia service quality, communication overhead efficiency and multimedia content integrity simultaneously. To provide robust video authentication while keeping bandwidth resource constraints, a novel SAP based network resource allocation scheme is proposed to improve energy efficiency and communication resource utilization in IPMN by jointly exploring the diversities in the source, the authentication and the protocol categories. Results based on simulation studies demonstrate the effectiveness of the proposed SAP scheme in achieving resource efficiency, video quality and authentication robustness, simultaneously.**

***Index Terms*—Inter-Planetary Multimedia Network, Stream Authentication, Efficiency**

## I. Introduction

The rapid growth of security sensitive multimedia content generated by various human explorations on the outer space, such as the Mars Exploration, has brought challenges on the current deep-space network capacity and bandwidth[1][2]. Future Inter-Planetary Multimedia Networks (IPMN) will meet the demands of multimedia communication among the orbiters, space crafts and the relay station on planets.

In the bandwidth and energy constrained IPMN, each user is allocated with limited resource due to time-varying channel conditions. As shown in Figure 1, three factors should be carefully traded off to increase the video authentication quality while keeping to the resource limitations. Traditional authentication schemes regardless of network capacity fail to meet these objectives simultaneously. On one hand, the cost of video quantization and compression level is not guaranteed to satisfy the resource constraints while allocating secure data in the middle. On the other hand, offering data integrity in a fixed mode may cause blackouts in the IPMN without allocating proper bits in the network protocol domain in the time-varying lossy channel conditions. Therefore, efficient resource allocation schemes for high-quality authenticated stream delivery are desired to solve the current problems.

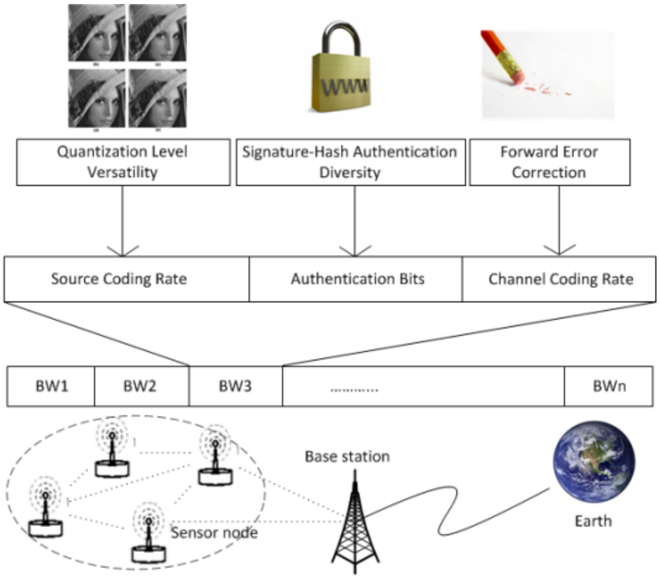


Figure 1 Resource-constrained source-authentication-channel optimization for IPMN

Recently, multimedia authentication is largely advanced in the research area. The authors in [3] found that current authentication mechanisms would have security risks after some nodes were compromised. To defend the attack, they divided the sensing area into several cells and also built a logical cell. The result shows a high security improve under this framework. In [4], the author proposed a collaborative transmission scheme to solve large sized image via wireless sensor network. In this paper, the limited resources and security requirement have been considered as conditions. By designing the approach without using any key distribution and management, they avoided any key management problem. Overlooking the security, the authors of [5] reported the security risk on current sensor platforms. Instead of focusing on securing the propagation of code images, the author proposes a sequence of light weight techniques to reduce the risk. The research in [6] focused on end-to-end media authentication schemes, and proposed a quality-optimized authentication algorithm. Using the packet success decode and authenticate rate, they found the quality of the authenticated media to optimize the transmit performance. Focusing on the base station model, [7] investigated three authentication schemes and proposed their own user based authentication schemes. By using identity-bit commitment, this new scheme overcomes the problems in current authentication scheme. In [8], the authors put forward a rate-distortion-authentication (R-D-A) optimized streaming technique for H.264 video authentication and transmission. Based on the authentication dependency and packet-level visual importance, the end to end distortion of authenticated video content is minimized. The researchers of [9] proposed an authentication resource allocation scheme for secure wireless multimedia streaming by joint considering the multimedia authenticity and energy consumption. A link-layer energy-distortion hash chain in JPEG 2000 streaming is modeled in order to optimize the authenticated distortion reduction in energy budget constraints.

All the aforementioned works focus on the source rate control and authentication rate control, without considering the network protocol overhead control. To the best of our knowledge, there is no such study, in the literature, about trading off the source coding rate, the authentication rate and the network protocol overhead. In contrast, we propose a simplified network resource allocation scheme named SAP (Source-Authentication-Protocol) to provide secure multimedia content delivery while keeping to limited bits-resource constraints in IPMN.

TABLE I
SUMMARY OF THE KEY NOTATIONS USED IN THE EQUATIONS

| SYMBOL | QUANTITY |
|---|---|
| $N$ | Number of frames in the sequence of video stream |
| $sr$, $au$, $pr$ | The category of video source coding, stream authentication, network protocols respectively. |
| $L_{sr\_i}$, $L_{au\_i}$, $L_{pr\_i}$, | The communication rate overhead of each packet for source coding rate, authentication rate, and network protocols |
| $\theta i$, $\delta i$, $\phi i$ | Physical layer transmission data rate for data packets |
| $R_s$ | Transmission bit rate overhead |
| $B_{max}$ | Total bit-allocation budget |
| $e$ | Bit error rate of a communication link |
| $\rho_f$ | Frame error rate of every frame in the video stream |
| $M$ | The number of bits of redundancy in the FEC scheme |
| $K$ | The number of bits of original data stream in a packet |
| $\Phi$ | The dependency flag |
| $\Delta D^l_i$ | The distortion reduction brought by $l$-th quantization level in the $i$-th frame of the reconstructed video |

The paper is organized as follows. In Section II, a framework of the mathematical resource allocation optimization model is formulated with bits-budget constraint. In Section III, the trade-offs between the source coding rate, the authentication rate and the network protocol overhead is analyzed in details. In Section IV, we propose the algorithm to solve this optimization problem. Section V shows the simulation results and studies the performance analysis of relevant cases. The conclusion is drawn in Section VI. Table I shows the notations and major symbols used in equations defined in this paper.

## II. MATHEMATIC PROBLEM FORMULATION

The overall problem can be formulated into a cross-layer pattern to optimize the secure multimedia content quality with resource efficiency guarantees. The objective of our work is to jointly optimize three parameter categories including video coding (sc), stream authentication (au), and network protocol overhead (pr) in order to achieve the best effort authentication video quality, e.g. to maximize the expected total distortion reduction ($E[\Delta D]$), by the optimal allocation of quantization level, authentication dependency and FEC redundancy bits.

$$\{(sr)_i,(au)_i,(pr)_i\}_{i\in[0,\dots,N-1]} = \mathrm{argmax}\,\{E[\Delta D]\} \qquad (1)$$

subject to the total bit resource budget constraint:

$$R_s \le B_{max} \qquad (2)$$

where $R_s$ denotes the total transmission bit rate overhead, $B_{max}$ denotes the bit-allocation budget. In the following sections, we will discuss how to solve the cross-layer resource allocation optimization problem in details.

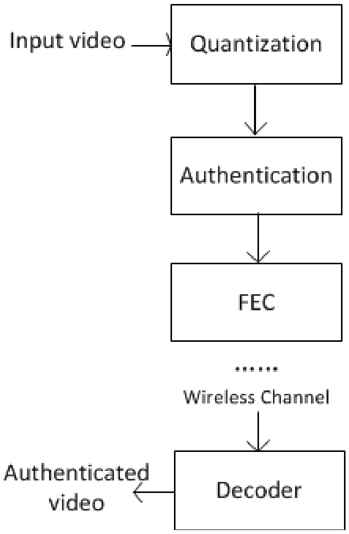


Figure 2 System diagram for source-authentication-channel optimized video transmission

## III. RESOURCE ALLOCATION ANALYSIS WITH SOURCE-AUTHENTICATION-PROTOCOL RATE OPTIMALITY

The goal of this cross-layer problem is to maximize the end-to-end distortion, i.e. the expected video authentication quality. In this paper, we define the authenticated video quality to be the distortion reduction (calculated in terms of the PSNR of Y, the luma component, in the YUV color space) summation of each frame in the video sequence that can be decoded and verified at the receiver. Let $\Delta D^l_i$ denote the distortion reduction brought by $l^{th}$ quantization level in the $i^{th}$ frame of the reconstructed video, $N$ denote the number of total frames in the sequence of video stream, $\rho_f$ denote the communication error probability of each frame, $\rho_a$ denote the authentication error probability of each frame, and $\rho_s$ denote the error probability of its dependent predecessor frame. $\Phi$ is the dependency flag, where 1 means the verification is also dependent on its proceeding authenticated frame and 0 means it is signed with an independent signature. The expectation of the total authenticated distortion reduction can be expressed as:

$$E[D]=\sum_{i=0}^{N-1}\Delta D_i^l(1-\rho_f)(1-\rho_a)(1-\rho_s\phi) \tag{3}$$

The resource consumption of the sequence of video stream, e.g., the summation of the communication rate overhead of every frame for source coding rate $L_{sr\_i}$, extra authentication rate $L_{au\_i}$ and communication protocol $L_{pr\_i}$, is calculated as follows:

$$R_s=\sum_{i\in[0,..,N-1]}L_{sr\_i}+L_{au\_i}+L_{pr\_i} \tag{4}$$

In this paper, the authenticated video is defined as a sequence of stream reconstructed and verified from received packets. As illustrated in Figure 2, at the sender, video stream is quantified, signed and protected before transmitting. To reconstruct the secure multimedia content at the receiver side, the sequence of video stream must be decoded and verified by authentication after the packets delivery. In the following three subsections, the contribution of distortion reduction and bit consumption of the three categories is discussed.

### A. Source coding rate

The different quantization levels will cause different distortion reductions. Intuitively, high quantization levels will improve the video quality and reduce video quantization distortion. Meanwhile, it will also bring large bit rate consumption. In this paper we adopt five different levels of quantization to count as different source coding rates.

### B. Authentication rate

All packets received should be verified by its corresponding signature or hash packets for authentication in secure wireless multimedia networks. Signature packets can be independently authenticated while hash packets should also be verified by its proceeding signature packet. If the signature packet is lost or unverified, the content packets that point to the leading packet are discarded as useless even though they are received successfully. So, the verification probabilities can be improved by increasing the number of frames followed with signature packets. However, this will also increase the overhead size. Note that the computing of a 2048-bits signature is much more complex than that of a hash, which usually takes 128 bits.

In this paper, we examine five different authentication modes in the Simple Hash Chain authentication graph (AP) [11]. The interval of hashes between every two signatures is increased by two each time, e.g. SISI, SIIISIII, …, SIIIIIIIISIIIIIIII.

### C. Communication Protocol overhead

The frame error rate is directly related to packet error rate. But in a very lossy channel, packet rate can be very high. For example, it can be as high as 10e-1 in the deep space environment. For such poor channel condition, most packets cannot be recovered after receiving. To ensure the reliability of the multimedia content at the receiver end, some channel coding technique should be considered in data transmission. Forward Error Correction (FEC) is applied in this paper, which introduces extra redundancy codes into the raw data to overcome the high bit error rate. In such way, some bit errors in the packets do not necessarily cause the packet error, protecting the data from corruption. Therefore, the FEC technique ensures a satisfying success rate of data transmission in very lossy channel conditions. Let $e$ denote the bit error rate, according to [10], the packet loss ratio $\rho$ can be calculated as

$$\rho=\sum_{i=M+1}^{M+K}C_{M+K}^{i}e^{i}(1-e)^{M+K-i} \tag{5}$$

where $C$ is the combination function. As the equation shows, the packet loss ratio is expressed as the summation of all possibilities of combinations of different bit errors and bits successes, with $i$ initialized from $M+1$ which means that a packet is considered as lost when the number of bit errors is larger than the redundancy bit. By applying FEC to original multimedia stream code before transmission, we can improve the quality performance of data delivery in the channel links of deep space networks.

In the next section, we will propose our algorithm to solve this cross-layer resource allocation problem.

*Algorithm 1 Optimized Transmission Strategy of Source-Authentication-Protocol*

```
1.  Read Input: $N, e, B_{max}$.
2.  Pre-calculate the expected distortion reduction and total
    bits consumption.
3.  Evaluate the bit rate overhead $R$ according to the budgets,
    and determine the optimized output.
    for j=1:3; // FEC
        for k=1:5; //Quantization
            for l=1:5; //Authentication
                If $D>D_{opt}$ and $R<B_{max}$ then,
                 Record the optimal value and strategy.
            End
        End
    End
4.  Output: $D_{opt}$ and $\{\theta_i, \delta_i, \phi_i\}$ | i=[0…,N-1] accordingly.
```

## IV. Algorithm Design

As mentioned in earlier sections, there are three transmission categories in a video stream to be optimized according to different bandwidth resource budgets. Let $\boldsymbol{\theta_i}$, $\boldsymbol{\delta_i}$, $\boldsymbol{\phi_i}$ denote the video quantization mode, authentication mode and channel coding mode of each frame in the video respectively. To obtain the optimized transmission strategy, e.g. a combination of these three modes, we propose a two-step algorithm to solve this optimization problem.

We first analyze for any given input video content, in order to get the bits frame and distortion reduction of every frame in the video sequence. Based on the data acquired in the pre-processing step, we then solve this optimization problem by applying a global searching algorithm, which is computationally intensive with a complexity of O($3^N$). Algorithm 1 describes the details of the source-authentication-protocol optimization process: how to determine the optimal transmitting strategy adaptively to resource budget and wireless channel conditions. Simulation

In this section, we provide simulation studies to demonstrate the effectiveness of the optimized SAP transmission resource allocation scheme over traditional schemes. The standard "akiyo" sample video sequence (30 frames in total with a configuration of 358×288 pixels for frame width and height) is encoded using H.264/AVC reference software JM 10.2 [12], where the distortion reduction of each frame and bit consumption is calculated. For convenience of discussion, each GOP comprises of I-frames only since our scope is focused on the media quality of stream-based authentication. As mentioned earlier, there are five different quality levels in the coded source stream with quantization parameters 50, 40, 30, 20, and 10. For authentication, we use 1024-bit signature and 128-bit hash to construct the diversity based on the Simple Hash Chain AP, where signatures are amortized among 2, 4, 6, 8 and 10 consecutive hashes. On the network protocol side, the FEC redundant bits in a packet are set to 1, 2, and 3 bits, respectively. In simulated secure multimedia wireless communication networks environment, the default communication link bit error rate is 1e-3. Several scenarios of the total communication bit budget are simulated, ranging from 0 to 700000 bits.

The proposed approach is denoted as "Optm", representing the optimized transmitting strategy for the communication resource allocation. For comparison, two traditional fixed resource allocation approaches that maximize and minimize the overhead of each category are denoted as "TradMax" and "TradMin".

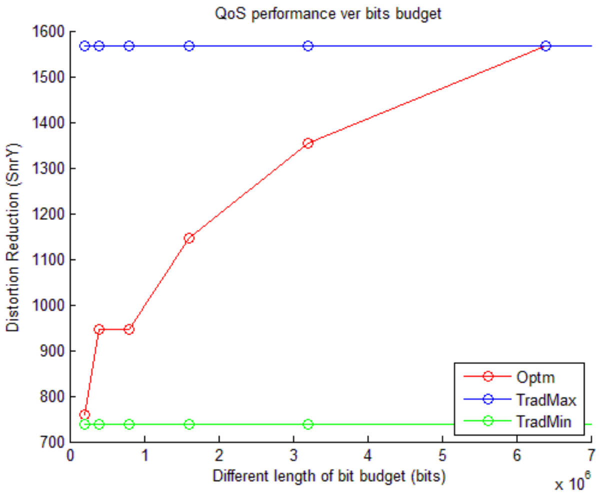
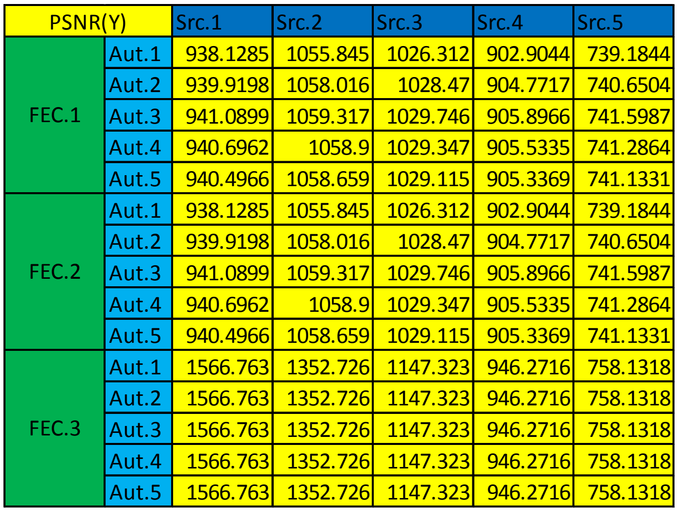


Figure 3 Video authentication quality performance under different budgets

Figure 3 shows the end-to-end authenticated video quality under different length of bit budgets. We can see that the TradMax approach which allocates the largest resource in the three pre-set modes on each transmission, regardless of the length of bit budgets, achieves the best packet delivery quality. However, the communication overhead of this fixed scheme is not suitable for time-varying wireless channel conditions. Similarly, the TradMin approach meets most of the bit budgets but offers the poorest video authentication quality every time. In contrast, the video authentication quality is adaptively increasing with the increasing length of bit budgets, always making the best use of the limited network resource.



| PSNR(Y) | | Src.1 | Src.2 | Src.3 | Src.4 | Src.5 |
|---|---|---|---|---|---|---|
| FEC.1 | Aut.1 | 938.1285 | 1055.845 | 1026.312 | 902.9044 | 739.1844 |
| | Aut.2 | 939.9198 | 1058.016 | 1028.47 | 904.7717 | 740.6504 |
| | Aut.3 | 941.0899 | 1059.317 | 1029.746 | 905.8966 | 741.5987 |
| | Aut.4 | 940.6962 | 1058.9 | 1029.347 | 905.5335 | 741.2864 |
| | Aut.5 | 940.4966 | 1058.659 | 1029.115 | 905.3369 | 741.1331 |
| FEC.2 | Aut.1 | 938.1285 | 1055.845 | 1026.312 | 902.9044 | 739.1844 |
| | Aut.2 | 939.9198 | 1058.016 | 1028.47 | 904.7717 | 740.6504 |
| | Aut.3 | 941.0899 | 1059.317 | 1029.746 | 905.8966 | 741.5987 |
| | Aut.4 | 940.6962 | 1058.9 | 1029.347 | 905.5335 | 741.2864 |
| | Aut.5 | 940.4966 | 1058.659 | 1029.115 | 905.3369 | 741.1331 |
| FEC.3 | Aut.1 | 1566.763 | 1352.726 | 1147.323 | 946.2716 | 758.1318 |
| | Aut.2 | 1566.763 | 1352.726 | 1147.323 | 946.2716 | 758.1318 |
| | Aut.3 | 1566.763 | 1352.726 | 1147.323 | 946.2716 | 758.1318 |
| | Aut.4 | 1566.763 | 1352.726 | 1147.323 | 946.2716 | 758.1318 |
| | Aut.5 | 1566.763 | 1352.726 | 1147.323 | 946.2716 | 758.1318 |

Figure 4 Results of QoS performance of the proposed SAP scheme (under bandwidth budgets 1600000 bits)

Figure 4 shows the numerical results of the distortion reduction of every possible combination of three communication categories in the pre-processed step of our proposed scheme. From analyzing the results in the table, it can be noted that by adding more FEC redundancy bits we can largely increase the video quality gain, since the successful frame delivery probability is largely increased. Also when we add 3 bits into the raw source authenticated video stream, we will always get the highest PSNR in spite of the other two categories, which implies the FEC channel coding overhead has a larger contribution to the video authentication delivery quality.

Another interesting point that caught our attention is that, intuitively, the higher quantization level we choose in the source coding side, the finer are the images in each frame, yielding higher PSNR of the video sequence. However, as shown in Figure 4, under the FEC 1 and FEC 2 scenarios, the PSNR value of Src. 1 is lower than that of Src. 2. The reason is that higher quantization levels also bring larger packet numbers in the source codestream. With low packet successful rate the frame successful rate will be even lower, thus the total PSNR of frame will decrease.

## V. Conclusion

In this paper we proposed a new scheme for improving video authentication quality with limited communication bandwidth.

The source coding, authentication diversity and channel coding were jointly studied to provide secure wireless multimedia communication in poor channel conditions in the IPMN. It is worth noting that more FEC redundancy codes and the highest quantization level are not needed for yielding QoS performance. Compared to the other two categories, the FEC contributes more to the successful transmission probability in the poor channel conditions while consuming less bit budget. Finally, a bit allocation scheme is proposed to optimize the transmission quality of authenticated multimedia content. Simulation results show that the proposed scheme achieves a significant higher distortion reduction than fixed transmission strategy.

## ACKNOWLEDGMENT

This research was supported in part by NASA EPSCoR MSI Faculty Engagement Competition grant NNX12AI13A on wireless networks, and South Dakota State University Research Scholarship Support Fund.

## REFERENCES

[1] Burleigh, S., Cerf, V., Durst, R., Fall, K., Hooke, A., Scott, K., & Weiss, H. (2002, January). The InterPlaNetary Internet: a communications infrastructure for Mars exploration. In IAF abstracts, 34th COSPAR Scientific Assembly (Vol. 1, p. 700).

[2] Akan, O.B.; Jian Fang; Akyildiz, I.F.; , "TP-planet: a reliable transport protocol for interplanetary Internet," *Selected Areas in Communications, IEEE Journal on* , vol.22, no.2, pp. 348- 361, Feb. 2004.

[3] Cungang Yang; Jie Xiao; , "Location-Based Pairwise Key Establishment and Data Authentication for Wireless Sensor Networks," Information Assurance Workshop, 2006 IEEE , vol., no., pp.247-252, 21-23 June 2006

[4] Honggang Wang; Dongming Peng; Wei Wang; Sharif, H.; Hsiao-Hwa Chen; , "Image transmissions with security enhancement based on region and path diversity in wireless sensor networks," Wireless communications, IEEE Transactions on , vol.8, no.2, pp.757-765, Feb. 2009

[5] An Liu; Peng Ning; Wang, C.; , "Lightweight Remote Image Management for Secure Code Dissemination in Wireless Sensor Networks," INFOCOM 2009, IEEE , vol., no., pp.1242-1250, 19-25 April 2009

[6] Qibin Sun; Apostolopoulos, J.; Chang Wen Chen; Shih-Fu Chang; , "Quality-Optimized and Secure End-to-End Authentication for Media Delivery," Proceedings of the IEEE , vol.96, no.1, pp.97-111, Jan. 2008

[7] Jamil, N.; Sameon, S.S.; Mahmood, R.; , "A User Authentication Scheme Based on Identity-bits Commitment for Wireless Sensor Networks," Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on , vol., no., pp.61-66, 22-23 Sept. 2010

[8] Zhishou Zhang; Qibin Sun; Wai-Choong Wong; Apostolopoulos, J.; Wee, S.; , "Rate-Distortion-Authentication Optimized Streaming of Authenticated Video," Circuits and Systems for Video Technology, IEEE Transactions on , vol.17, no.5, pp.544-557, May 2007

[9] Wei Wang; Dongming Peng; Honggang Wang; Sharif, H.; Hsiao-Hwa Chen; , "Energy-Distortion-Authentication Optimized Resource Allocation for Secure Wireless Image Streaming," Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE , vol., no., pp.2810-2815, March 31 2008-April 3 2008

[10] B.Sklar, *Digital Communications,* 2$^{nd}$ ed., Prentice Hall

[11] Gennaro, Rosario, and Pankaj Rohatgi. "How to sign digital streams." Advances in Cryptology—CRYPTO'97 (1997): 180-197.

[12] Tourapis, Alexis Michael, Athanasios Leontaris, K. Suhring, and Gary Sullivan. "H. 264/14496-10 AVC reference software manual." Doc. JVT-AE010 (2009).