

## Verification of the Integrity and Legitimacy of Academic Credential Documents in an International Setting

BY GEORGE D. GOLLIN

The global demand for higher education currently exceeds the world's existing university capacity. This shortfall is likely to persist for the foreseeable future, raising concerns that frustrated students might choose to purchase fraudulent credentials from counterfeiters or diploma mills. International efforts to encourage the development of reliable, authoritative lists of recognized universities are currently underway.<sup>1</sup> An employer might use such lists and related databases to determine the legitimacy of a school attended by a prospective employee. But an additional approach to credential authentication is possible in which degree verification is performed automatically using the same information security tools that permit secure financial transactions to proceed over open communication networks. It is possible that the development of reliable databases (which require active engagement in order to be useful) in combination with a widely adopted standard for self-authenticating academic documents could drive nearly all counterfeiters and diploma mills out of business.

Public-key cryptography can provide a technical solution to the problem of authenticating academic documents such as transcripts and diplomas. When combined

with an appropriate system to manage universities' public keys (so that only legitimate universities are issued keys by a "certificate authority"), it becomes possible to determine whether a document is genuine or counterfeit, and also whether or not it was issued by a legitimate postsecondary institution rather than a diploma mill.

Interesting lessons can be learned from the history of efforts to suppress fraud in financial transactions. After discussing these, I describe a model for the generation of secure, verifiable diplomas and transcripts.

### PAPER CURRENCY, PAPER DOCUMENTS

In 1860, at the beginning of the United States' Civil War, the manufacture of American currency was managed separately by each state in the Union. Because there was no national coordination of the design of coins and bills, it was difficult for a bank in one state to recognize as illegitimate counterfeit bills that purported to be the legal currency of a different state (NARA 1998). It is estimated that one-third to one-half of the currency in circulation in the United States at the time was counterfeit (USSS 2009).

### Suppression of Counterfeit Currency

On the last day of his life, President Abraham Lincoln ordered Secretary of the Treasury Hugh McCulloch to ad-

<sup>1</sup> See, for example, the UNESCO Portal on Higher Education Institutions, available online at <[http://portal.unesco.org/education/en/ev.php-URL\\_ID=49864&URL\\_DO=DO\\_TOPIC&URL\\_SECTION=201.html](http://portal.unesco.org/education/en/ev.php-URL_ID=49864&URL_DO=DO_TOPIC&URL_SECTION=201.html)>.

**(ORIGINAL ADVERTISEMENT REMOVED)**

**(ORIGINAL ADVERTISEMENT REMOVED)**

dress this problem. McCulloch created the United States Secret Service in response to the President's charge (USSS 2009). Though better known now for its mission protecting government officials and foreign diplomats, the Secret Service, for the remainder of the nineteenth century, had currency fraud as its primary focus. The Service moved aggressively against the producers of counterfeit money, closing hundreds of production sites in only a few years and eventually reducing the fraction of U.S. currency in circulation that was counterfeit to well under one-tenth of one percent.

The availability of *intaglio* process currency printing presses (in spite of international controls meant to keep these out of the hands of counterfeiters), in combination with modern technology, has given rise to new lines of counterfeit notes that are nearly undetectable as fakes. The provenance of these "super notes" is not entirely clear, although the United States Treasury has stated that such notes are believed to be of North Korean origin (Mihm 2006). Thus, some of the concerns this raises are international and inherently political in scope. According to a North Korean defector, "Kim Jong I endorsed counterfeiting not only as a way of paying for covert operations but also as a means of waging economic warfare against the United States, 'a way to fight America, and screw up the American economic system'" (Mihm 2006).

We expect that the use of counterfeit bills of one country's currency inside another country is a smaller problem than the use of counterfeits within the purported country of origin of the currency. Moreover, banks and exchange services that buy and sell foreign currency can be expected to train their staffs to reject suspicious or entirely unrecognized coins and bills. For example, it is unlikely that a bank in France would mistakenly issue euros in exchange for Seborgan luigini.<sup>2</sup> As a result, economic hazards associated with the production of currency for an imaginary country like Seborga are almost certainly minimal.

An inherent limitation in paper currency is the low level of scrutiny to which it can reasonably be subjected while

still preserving the anonymity of the bearer in casual financial transactions. Is it practical for a clerk in a grocery store to subject a customer's payment to a neutron scattering analysis? Central to the use of paper currency in small purchases is the absence of a trusted third party who verifies the currency's legitimacy. Consequently, paper currency can only be as robust against counterfeiting as allowed by countermeasures that can be embedded in individual coins and bills. If a merchant receives payment in unfamiliar currency (for example, from a foreign visitor hoping to use his/her national currency), the risk of fraud increases.

### Problems in Authenticating Paper Academic Documents

Many of the security issues concerning academic documents are similar to those relating to paper currency transactions. For example, a job candidate might be asked by a prospective employer to provide a transcript showing his university courses and grades. Without confirmation from a third party that the document is valid, how can the employer tell whether the transcript was actually produced by the university rather than by a counterfeiter? Legitimate printers use various kinds of security paper and special inks to make it more difficult to counterfeit their documents. But these also are used by counterfeiters: A high-quality counterfeit transcript, printed on security paper, can be purchased online for less than \$100.

An added complication with academic documents is the wide variation from school to school in transcript layout and printing technology. An employer typically is unfamiliar with the standard format of a transcript issued by a particular institution, just as a 19th century U.S. merchant in one state was unfamiliar with the legitimate currency of another state. Ultimately, it probably is more important for a counterfeit transcript to look *good* than for it to resemble a genuine transcript from the target school. The St. Regis diploma mill sold counterfeits of at least 77 legitimate schools' documents but made little effort to have such counterfeits conform to the layout and design utilized by those schools.<sup>3</sup>

An employer could ask a job applicant to have a transcript sent directly by the school's registrar, but this is at

<sup>2</sup> Seborga is a small community in the Ligurian region of Italy. Seborgan residents pay Italian taxes, vote in Italian elections, and receive the various public services provided to any Italian community by Italy. However, some of Seborga's inhabitants maintain that the town is not part of the Republic of Italy. The luigino, the Seborgan unit of currency, is generally accepted by merchants inside Seborga. The value of the luigino is pegged to the U.S. dollar at the rate of 1 luigino = \$6, making it the highest-valued unit of currency in Europe.

<sup>3</sup> United States Sentencing Memorandum, Government Exhibit A, United States of America, Plaintiff vs. Dixie Ellen Randock, Defendant, Case CR-05-180-1-LRS, United States District Court, Eastern District of Washington, June 5, 2008.

best a weak attempt at reducing the chance of receiving a counterfeit document. It is a simple matter to find a re-mailing service that, for a price, can receive a dishonest person's document and remail it from the same postal district as the university in question.

And what is to be done when a job applicant presents credentials from a diploma mill purportedly located abroad rather than providing counterfeit documents that bear the name of a legitimate school? "West Coast University (WCU)"<sup>4</sup> claims to have a campus in Seborga and to be accredited by the "Accreditation Council" of Seborga,<sup>5</sup> but a WCU degree has no more legitimacy outside the not-quite-real country of Seborga than the Seborgan luigino.

It is not practical to expect an academic document delivery system to be robust against determined efforts at fraud without introduction of a trusted third party to assist with verification. Ideally, the third party would confirm that the school named in the document had in fact generated the document, that the document had not been altered, and that the school held proper degree-granting authority according to the appropriate education ministry or state higher education office.

## **PUBLIC-KEY CRYPTOGRAPHY**

The invention in the 1970s of public-key cryptography provided the technical foundation necessary for secure financial transactions to proceed over non-secure communications networks. Using a public-key algorithm, an author can transmit encrypted information (such as a credit card number) over an open line to a reader such that only the reader (but no eavesdroppers who might intercept the transmission) can decrypt the information. The author and reader do not need to share private information, such as a secret decryption key, in order to effect the transmission.

In public-key cryptography, a document is scrambled by its creator using one *cryptographic key* so that it can be deciphered by its reader using a different key. The two keys are linked and are generated through use of a mathematical algorithm. The keys must be used together in order to encipher and then decipher the message. It is nearly impossible to determine the value of one key with knowledge of the value of the other key.

A participant in a secure transaction who wishes to receive a message will make one of the keys public, perhaps by posting it to the World Wide Web. The other key remains private. Anyone who wishes to send this participant an enciphered file will use the public key to scramble her message. The message can only be deciphered by someone in possession of the private key. By using the public key, anyone can send an encrypted message; but only the intended receiver can decrypt the message by using the private key that is paired with the public key.

## **Digital Signatures**

Public-key techniques also permit the creation of "digital signatures" so that a reader can authenticate an unencrypted document. The signer uses a private key to encipher his/her "signature" and transmits this with the document to a destined receiver. The signer's public key is freely available and is used by the receiver to decrypt the digital signature. As long as the signer actually did use the private key that is paired with the corresponding public key, the signature will decrypt properly.

The signature allows the reader to determine that the identity of the author of the document is the same as that of the person who created (and posted to the World Wide Web) the public key for her digital signature.

## **Use of Cryptographic Hash Functions to Verify Document Integrity**

A "hash function" generates something akin to a digital fingerprint for a document. The function takes an input file of arbitrary length and generates an output of fixed length. The output changes dramatically with small changes to the input file, so that even the most minor modification will change the file's hash value significantly.

Often, a hash value is included with the signature information that is encrypted to create a digital signature. After a document is received and the digital signature decrypted, the document's hash value can be recalculated and compared with the value that was contained in the signature. If the hash values match, the document has not been altered.

## **Certificate authorities and trusted third parties**

Public-key algorithms by themselves can only guarantee the consistency of a document author's identity from doc-

<sup>4</sup> See <[http://westcoast-edu.com/locations\\_and\\_contacts.html](http://westcoast-edu.com/locations_and_contacts.html)>.

<sup>5</sup> See <[www.seborga-edu.info/Members.htm](http://www.seborga-edu.info/Members.htm)>

ument to document. For example, a digital signature on a document from the “National Board of Education” can assure a reader that something calling itself the National Board of Education really did create the document. It can’t, however, confirm that the “National Board of Education” is actually a board of education rather than something entirely different.<sup>6</sup>

It is necessary to involve a trusted third party in order to confirm that the merchant whose name is carried by the digital signature is not misrepresenting its identity. This verification service often is provided by a commercial “certificate authority” (CA) such as VeriSign. When a Web browser displays a page on which secure information is to be entered, the browser automatically contacts the appropriate CA. If the merchant’s identity and encryption key are known to the CA, the browser allows the transaction to proceed.

### Electronic Commerce

Applications of public-key cryptography to electronic commerce are obvious: A buyer can send credit card information to a seller without risk even as she is assured that the identity of the seller is as expected.

Forrester Research (2005), a market research company with headquarters in the United States, predicts that electronic commerce will account for 13 percent of U.S. retail sales by 2010, reaching an annual level of approximately \$329 billion. The commercial impact of technology that enables secure transactions is enormous.

### APPLYING E-COMMERCE SECURITY TOOLS TO ACADEMIC DOCUMENT AUTHENTICATION

The security problems associated with online credit card purchases are more complex than those associated with verification of academic documents. Whereas secure electronic commerce requires encryption of information sent over a network as well as authentication of a customer’s credit card, transcript security is primarily a matter of authentication: the transcript document should not have been modified since it was produced, and it must have been produced by a school with legitimate degree-granting authority.

A number of initiatives to adapt cryptographic techniques to the academic setting are in progress.<sup>7</sup> The methods used to create a verifiable transcript are simple, nearly unbreakable, and well-suited to documents for which delivery in electronic form (*i.e.*, as PDF—Portable Document Format—files) is acceptable.

It would be appropriate for all academic documents to include hashed digital signatures whose validity would be verified by a commercial certificate authority that would work with a central academic authority (such as a branch of UNESCO). By restricting the certificates to schools with legal degree-granting authority, this document verification system also would serve as a straightforward mechanism for excluding diploma mills.

When a prospective employer opens a PDF-format transcript that contains an embedded digital signature, the software that opens the document (typically Adobe Reader) opens a separate window informing the viewer of the certificate status of the document, making use of key, hash, and digital signature information. If the document is not from a legitimate school, the reading software will offer no verification of authenticity.

### A RECOMMENDATION

It is appropriate for UNESCO to advocate for adoption of an international electronic security standard for academic transcripts and diplomas. A branch of UNESCO (or some other trusted international academic agency) could and should partner with a commercial certificate authority provider to permit authentication of documents from legitimate postsecondary institutions.

Given progress in this direction, a first step would be to assess the current state of electronic transcript technology and to discuss with interested groups their plans for further development of their systems.

Intelligent management and dissemination of information concerning the legitimacy of higher education programs and credentials is one of the most effective tools to be used in the suppression of diploma mills. If employers were to come to expect that viewing a PDF transcript file should always produce an authentication message, they

<sup>6</sup> The “National Board of Education” was part of the St. Regis diploma mill, whose owners were convicted of U.S. criminal violations in 2008. (See material posted at <[www.hep.uiuc.edu/home/g-gollin/pigeons/#usss\\_sru](http://www.hep.uiuc.edu/home/g-gollin/pigeons/#usss_sru)>.)

<sup>7</sup> See, for example, Thomas Black, “Are We Ready for Another Change? Digital Signatures Can Change How We Handle the Academic Record,” *College and University*, 80,1:55, and Thomas Black, “A Case for Electronic Transcripts,” *College and University*, 82(2): 41.

might be more likely to identify a bogus transcript from a bogus school for what it is.

## REFERENCES

NARA. See National Archives and Records Administration.  
National Archives and Records Administration. 1998. The U.S. Secret Service in history. *Inside the White House*. Spring. Retrieved from: <<http://clinton4.nara.gov/WH/kids/inside/html/spring98-2.html>>.  
United States Secret Service. 2009. *Counterfeit Division* (web page). Retrieved May 5 from: <[www.ustras.gov/ussf/counterfeit.shtml](http://www.ustras.gov/ussf/counterfeit.shtml)>.  
USSS. See United States Secret Service.  
Mihm, S. 2006. No ordinary counterfeit. *New York Times Magazine*. July 23.

Forrester Research. 2005. *Forrester Research US eCommerce Forecast: Online Retail Sales to Reach \$329 Billion by 2010*. September 19, 2005. Available at: <[www.forrester.com/ER/Press/Release/0,1769,1033,00.html](http://www.forrester.com/ER/Press/Release/0,1769,1033,00.html)>.

## About the Author

**GEORGE GOLLIN** is Professor of Physics at the University of Illinois at Urbana-Champaign. As a faculty service activity, Gollin focuses on topics in international university accreditation with an emphasis on the problem of diploma mills. He serves on the board of directors of the Council for Higher Education Accreditation.

