Verification of the integrity and legitimacy of academic credential documents in an international setting

George D. Gollin
Department of Physics
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801 USA
g-gollin@illinois.edu

October 10, 2008

Introduction
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. An employer might use these 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.

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.

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.

There are interesting lessons to be learned from the history of efforts to suppress fraud in financial transactions. I discuss these and then describe a model for 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. Since there was no national coordination of the designs 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. It is estimated that

1 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.
one third to one half of the currency in circulation in the United States at the time was counterfeit.³

Suppression of counterfeit currency

On the last day of his life, Abraham Lincoln, sixteenth president of the United States, ordered Secretary of the Treasury Hugh McCulloch to address this problem. McCulloch created the United States Secret Service in response to the President’s charge.⁴ Though better known for its mission protecting government officials and foreign diplomats, currency fraud was the Service’s primary focus for the remainder of the nineteenth century. The Secret Service moved aggressively against the producers of counterfeit money, closing hundreds of production sites in only a few years, 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 they believe them to be of North Korean origin.⁵ Some of the concerns this raises are international, and inherently political in thrust. According to a North Korean defector, “Kim Jong Il 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.’”⁶

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 in-country. In addition, 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.⁷ As a result, economic hazards associated with the production of currency from an imaginary country like Seborga are almost certainly minimal.

⁴ Ibid.
⁵ Stephen Mihm, “No Ordinary Counterfeit,” New York Times Magazine, July 23, 2006. From Mihm’s article: “‘The North Koreans have denied that they are engaged in the distribution and manufacture of counterfeits, but the evidence is overwhelming that they are,’ Daniel Glaser, deputy assistant secretary for terrorist financing and financial crimes in the Treasury Department, told me recently. ‘There’s no question of North Korea’s involvement.’”
⁶ Ibid.
⁷ 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 actually not part of the Republic of Italy. In 1963 the Seborgan resident Giorgio Carbore declared Seborga independent of Italy since “he claimed, when the principality was sold to the Kings of Savoy and Sardinia in 1729, the sale was never properly recorded.” [Malcom Moore, “Battle rages for His Tremendousness's throne,” U.K. Daily Telegraph, June 13, 2006.] Carbore was then “elected” Sua Tremendità (“Your Tremendousness”) of Seborga by his fellow Seborgan. He continues to hold this local title. 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.
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. And 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 attached to paper currency transactions. For example, a job candidate might be asked by a prospective employer to provide a transcript showing his/her 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 a counterfeiter? Legitimate printers use various kinds of “security paper” and special inks to make it more difficult to counterfeit their documents. But these are also 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 school-to-school variation in transcript layout and printing technology. An employer will generally be unfamiliar with the format of a transcript that a job applicant provides, just as a 19th century U.S. merchant in one state might be unfamiliar with the legitimate currency from another state. It is probably 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 their fakes conform to the layout and design employed by those schools.

An employer could ask a job candidate to have a transcript sent directly from the school’s registrar. But this is at best a weak attempt at reducing the chance of receiving a counterfeit document. It is a simple matter to find a remailing service that can, for a price, receive a dishonest person’s document and remail it from the same postal district as the desired university.

And what is to be done when a job candidate 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” claims to have a campus in Seborga and to be accredited by the “Accreditation Council” of Seborga 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 help with verification. Ideally the third party would determine that the school named in the documents had actually generated the documents, that the documents had not been altered, and that the school held

---

9 http://westcoast-edu.com/locations_and_contacts.html
10 http://www.seborga-edu.info/Members.htm
proper degree granting authority, issued by the appropriate education ministry or state higher education office.

Public-key cryptography

The invention of public-key cryptography in the 1970’s created 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 in a fashion so 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. They must be used together in order to encipher, 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 worldwide web. The other key remains private. Anyone who wishes to send this participant an enciphered file will use the public key to scramble their 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 worldwide web) the public key for his/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 even the most minor of modifications 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 document 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, tell us whether the “National Board of Education” is actually a board of education, or something entirely different.\(^{12}\)

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 his/her identity. This verification service is often provided by a commercial “certificate authority” (CA) such as VeriSign. When a web browser displays a page in 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**

The applications to electronic commerce of public-key cryptography are obvious: a buyer can send credit card information to a seller without risk, while being assured that the identity of the seller is as expected.

Forrester Research, a market research company with headquarters in the United States, predicts that electronic commerce will comprise 13% of U.S. retail sales by 2010, reaching an annual level of approximately $329 billion.\(^ {13}\) (The 2005 U.S. online sales volume was $172 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—secure electronic commerce requires encryption of information sent over a network, as well as authentication of a customer’s credit card. The matter of transcript security is primarily one 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.

---

\(^{12}\) The “National Board of Education” was part of the St. Regis diploma mill. Its owners were convicted of U.S. criminal violations in 2008. See material posted at [http://www.hep.uiuc.edu/home/g-gollin/pigeons/#usss_sru](http://www.hep.uiuc.edu/home/g-gollin/pigeons/#usss_sru).

A number of initiatives to adapt cryptographic techniques to an academic setting are in progress.\textsuperscript{14} The methods used to create a verifiable transcript are simple, nearly unbreakable, and well-suited to documents for which delivery in electronic form (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 would also serve as a straightforward mechanism for the exclusion of 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 the key, hash, and digital signature information. If the document is not from a legitimate school there will be no verification of authenticity offered by the reading software.

\textit{A recommendation}

I believe it is appropriate for UNESCO to advocate that an international electronic security standard for academic transcripts and diplomas be adopted, and that a branch of UNESCO (or some other trusted international academic agency) partner with a commercial certificate authority provider to permit authentication of documents from legitimate postsecondary institutions.

In that there is already progress in this direction, a first step would be to assess the current state of electronic transcript technology and 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 came to expect that viewing a PDF transcript file should always produce an authentication message, they might be more likely to identify a bogus transcript from a bogus school for what it is.