健康保險資料庫與資訊安全

王柏堯

中央研究院資訊科學研究所

“Computer security is not privacy protection”

“An area that might appear to have a common ancestry with the subject of this paper is access control and authentication, which are traditional areas associated with computer security. Work in this area ensures that the recipient of information has the authority to receive that information. While access control and authentication protections can safeguard against direct disclosures, they do not address disclosures based on inferences that can be drawn from released data. The more insidious problem in the work that is the subject of this paper is not so much whether the recipient can get access or not to the information as much as what values will constitute the information the recipient will receive. A general doctrine of the work presented herein is to release all the information but to do so such that the identities of the people who are the subjects of the data (or other sensitive properties found in the data) are protected. Therefore, the goal of the work presented in this paper lies outside of traditional work on access control and authentication.”

背景

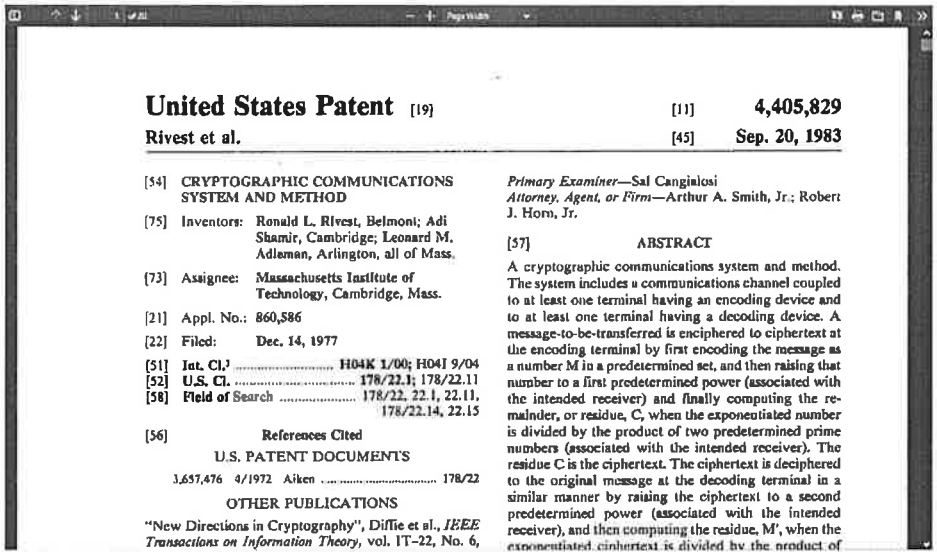
- 健康保險資料於釋出前，將可識別個人之欄位（如姓名、身份證字號）進行多次加密。
  - 加密：將原始資料改寫，使他人無法自改寫後的資料推測原始資料之內容。
  - 解密：將改寫後的資料回覆成原始資料。
- 加密與解密為資料安全中常利用之技術。
- 因為可識別個人欄位經過加密，他人無法自改寫後的欄位推測原始內容，故無法由這些改寫後的欄位識別個人。
- 利用資訊安全技術，保障個人隱私。

密碼系統與密碼程式

- 加密與解密皆為密碼系統所提供之操作。
- 這些操作實務上以密碼程式進行。
- 健康保險資料庫中的加密動作，便是執行密碼程式。
- 這些密碼程式的來源為何？

密碼系統

- 過去數十年，密碼學家提出了許多的密碼系統。
- 當密碼系統被發現後，密碼學家會公開密碼系統的細節。



United States Patent [19]

Rivest et al.

[11] **4,405,829**

[45] **Sep. 20, 1983**

[54] CRYPTOGRAPHIC COMMUNICATIONS SYSTEM AND METHOD

[75] Inventors: Ronald L. Rivest, Belmont; Adi Shamir, Cambridge; Leonard M. Adleman, Arlington, all of Mass.

[73] Assignee: Massachusetts Institute of Technology, Cambridge, Mass.

[21] Appl. No.: 860,586

[22] Filed: Dec. 14, 1977

[51] Int. Cl.³ H04K 1/00; H04I 9/04

[52] U.S. Cl. 178/22.1; 178/22.11

[58] Field of Search 178/22, 22.1, 22.11, 178/22.14, 22.15

[56] References Cited

U.S. PATENT DOCUMENTS

3,657,476 4/1972 Aiken 178/22

OTHER PUBLICATIONS

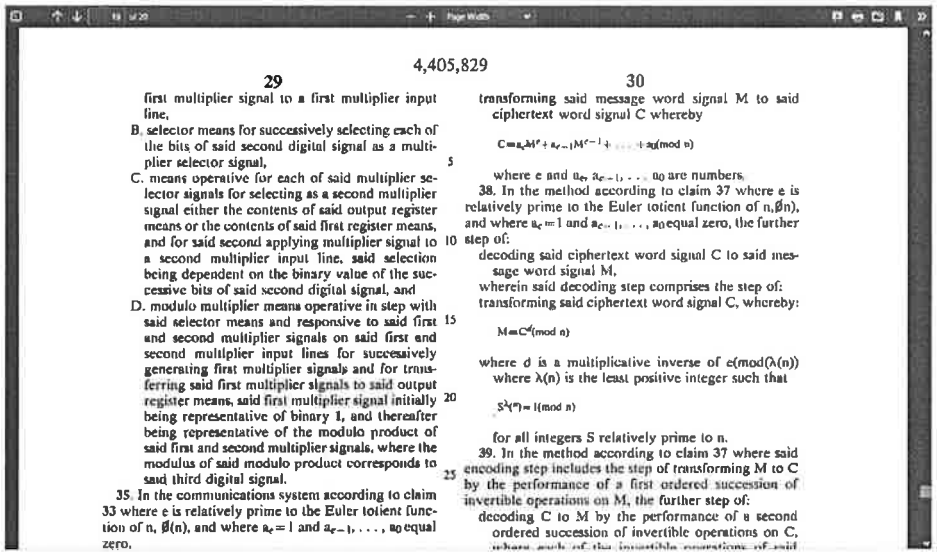
"New Directions in Cryptography", Diffie et al., *IEEE Transactions on Information Theory*, vol. IT-22, No. 6,

Primary Examiner—Sal Cangialosi

Attorney, Agent, or Firm—Arthur A. Smith, Jr.; Robert J. Horn, Jr.

[57] ABSTRACT

A cryptographic communications system and method. The system includes a communications channel coupled to at least one terminal having an encoding device and to at least one terminal having a decoding device. A message-to-be-transferred is enciphered to ciphertext at the encoding terminal by first encoding the message as a number M in a predetermined set, and then raising that number to a first predetermined power (associated with the intended receiver) and finally computing the remainder, or residue, C, when the exponentiated number is divided by the product of two predetermined prime numbers (associated with the intended receiver). The residue C is the ciphertext. The ciphertext is deciphered to the original message at the decoding terminal in a similar manner by raising the ciphertext to a second predetermined power (associated with the intended receiver), and then computing the residue, M', when the exponentiated ciphertext is divided by the product of



first multiplier signal to a first multiplier input line,

B. selector means for successively selecting each of the bits of said second digital signal as a multiplier selector signal,

C. means operative for each of said multiplier selector signals for selecting as a second multiplier signal either the contents of said output register means or the contents of said first register means, and for said second applying multiplier signal to a second multiplier input line, said selection being dependent on the binary value of the successive bits of said second digital signal, and

D. modulo multiplier means operative in step with said selector means and responsive to said first and second multiplier signals on said first and second multiplier input lines for successively generating first multiplier signals and for transferring said first multiplier signals to said output register means, said first multiplier signal initially being representative of binary 1, and thereafter being representative of the modulo product of said first and second multiplier signals, where the modulus of said modulo product corresponds to said third digital signal.

35. In the communications system according to claim 33 where e is relatively prime to the Euler totient function of n, $\phi(n)$, and where $a_e = 1$ and $a_{e-1}, \ldots, a_0$ equal zero.

transforming said message word signal M to said ciphertext word signal C whereby

$$C = a_e M^e + a_{e-1} M^{e-1} + \ldots + a_0 \pmod{n}$$

where e and $a_e, a_{e-1}, \ldots a_0$ are numbers.

38. In the method according to claim 37 where e is relatively prime to the Euler totient function of n, $\phi(n)$, and where $a_e = 1$ and $a_{e-1}, \ldots, a_0$ equal zero, the further step of:

decoding said ciphertext word signal C to said message word signal M,

wherein said decoding step comprises the step of:

transforming said ciphertext word signal C, whereby:

$$M = C^d \pmod{n}$$

where d is a multiplicative inverse of $e \pmod{\lambda(n)}$ where $\lambda(n)$ is the least positive integer such that

$$S^{\lambda(n)} = 1 \pmod{n}$$

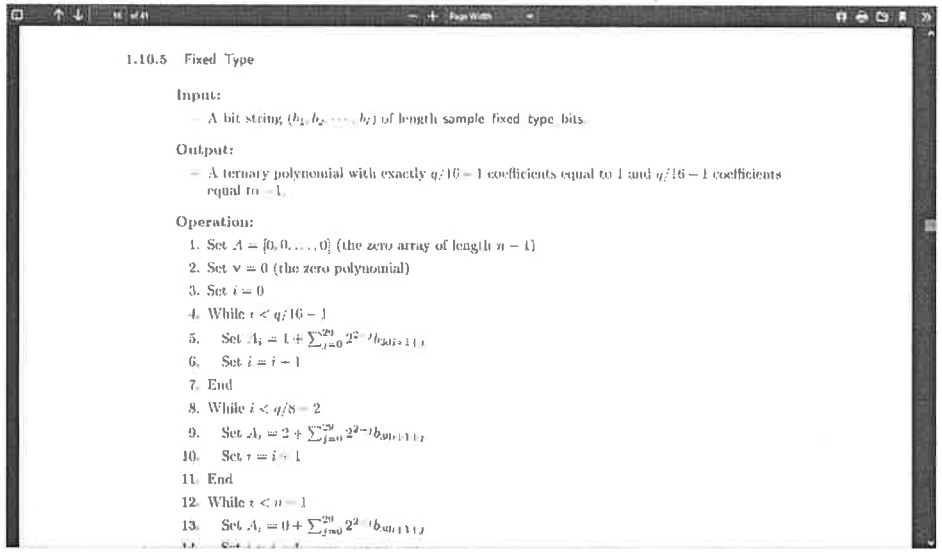
for all integers S relatively prime to n.

39. In the method according to claim 37 where said encoding step includes the step of transforming M to C by the performance of a first ordered succession of invertible operations on M, the further step of:

decoding C to M by the performance of a second ordered succession of invertible operations on C,

密碼系統

- 根據公開的密碼系統，解密專家嘗試找到密碼系統的漏洞。
- 經過密碼學家與解密專家檢視後，密碼系統才有初步的安全性。



1.10.5 Fixed Type

Input:

– A bit string $(b_1, b_2, \ldots, b_l)$ of length sample_fixed_type_bits.

Output:

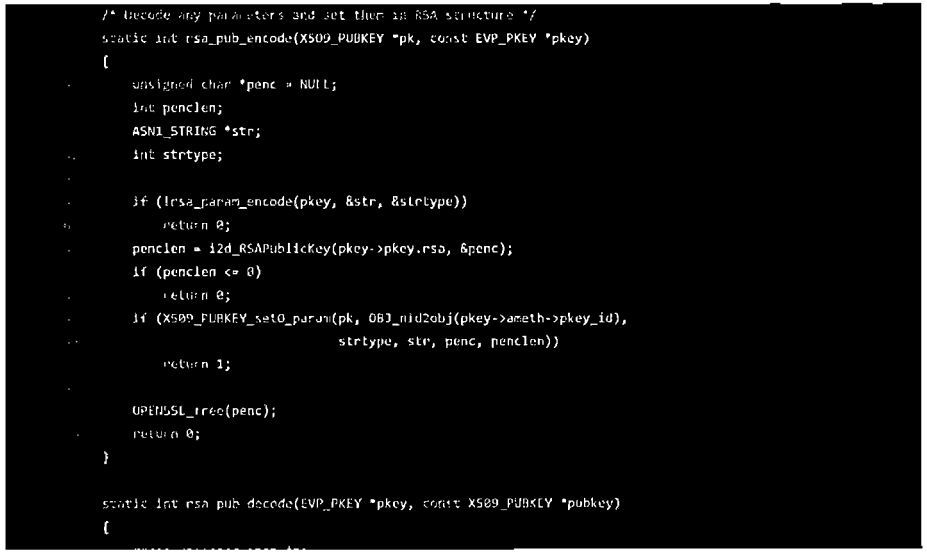
– A ternary polynomial with exactly $q/16-1$ coefficients equal to 1 and $q/16-1$ coefficients equal to -1.

Operation:

1. Set $A = \{0, 0, \ldots, 0\}$ (the zero array of length $n-1$)
2. Set $v = 0$ (the zero polynomial)
3. Set $i = 0$
4. While $i < q/16 - 1$
5. Set $A_i = 1 + \sum_{j=0}^{29} 2^j b_{30i+j}$
6. Set $i = i + 1$
7. End
8. While $i < q/8 - 2$
9. Set $A_i = 2 + \sum_{j=0}^{29} 2^j b_{30i+j}$
10. Set $i = i + 1$
11. End
12. While $i < n - 1$
13. Set $A_i = 0 + \sum_{j=0}^{29} 2^j b_{30i+j}$

密碼程式

- 密碼程式設計師為密碼系統編寫程式，並公開供大眾檢視。
- 這些密碼程式才是進行加密操作的主體。

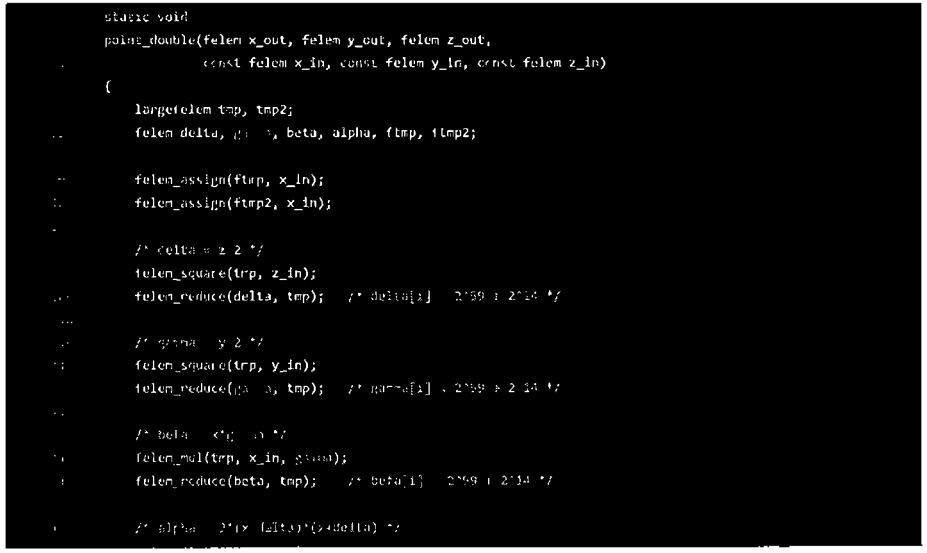


```
/* Decode any parameters and set them in RSA structure */
static int rsa_pub_encode(X509_PUBKEY *pk, const EVP_PKEY *pkey)
{
    unsigned char *penc = NULL;
    int penclen;
    ASN1_STRING *str;
    int strtype;

    if (!rsa_param_encode(pkey, &str, &strtype))
        return 0;
    penclen = i2d_RSAPublicKey(pkey->pkey.rsa, &penc);
    if (penclen <= 0)
        return 0;
    if (X509_PUBKEY_set0_param(pk, OBJ_nid2obj(pkey->ameth->pkey_id),
                               strtype, str, penc, penclen))
        return 1;

    OPENSSL_free(penc);
    return 0;
}

static int rsa_pub_decode(EVP_PKEY *pkey, const X509_PUBKEY *pubkey)
{
```



```
static void
point_double(felem x_out, felem y_out, felem z_out,
             const felem x_in, const felem y_in, const felem z_in)
{
    largefelem tmp, tmp2;
    felem delta, gamma, beta, alpha, ftmp, ftmp2;

    felem_assign(ftmp, x_in);
    felem_assign(ftmp2, x_in);

    /* delta = z^2 */
    felem_square(tmp, z_in);
    felem_reduce(delta, tmp);   /* delta[i] < 2^59 + 2^14 */

    /* gamma = y^2 */
    felem_square(tmp, y_in);
    felem_reduce(gamma, tmp);   /* gamma[i] < 2^59 + 2^14 */

    /* beta = x*gamma */
    felem_mul(tmp, x_in, gamma);
    felem_reduce(beta, tmp);    /* beta[i] < 2^59 + 2^14 */

    /* alpha = 3*(x-delta)*(x+delta) */
```

公開檢視與資訊安全

- 密碼學家設計密碼系統時，需要數學推論。
- 讓解密專家檢視密碼系統，可以減少數學推論的錯誤。
- 密碼程式設計師編寫密碼程式時，必須精確地實現密碼系統。
- 讓專家檢視密碼程式，可以減少程式編寫的錯誤。
- 即使是密碼學家或密碼程式設計師，也無法保證自己不犯錯。
  - 後量子密碼系統標準中，因被解密專家破解而退出之徵選者。
  - 研究中找到密碼程式的錯誤。
  - 美國國家標準局人員邀請專家進行虛擬會談，分享增加密碼程式安全性之經驗。

衛生福利部資料庫之密碼系統與程式

- （以下空白）

認證與資訊安全

- 認證是管理的一種手段。
- 經由形式上符合規範的操作，期望達到實質上的效果。
- 形式上的安全認證，從來就無法保證實質上的資訊安全。

新聞

英飛凌TPM晶片爆安全漏洞，Google、微軟忙修補

CRoCS發現英飛凌的TPM韌體有一演算法漏洞，可能產生脆弱的RSA金鑰，若駭客知公鑰，可能因此計算出私鑰，影響英飛凌自2012年以來推出的TPM晶片，包括英飛凌、Google、微軟、聯想、HP、富士通等業者已開始修補。

The foundations of "Fast Prime" date back to the year 2000. Its use started around ten years later after thorough reviews. As a sub-part of one cryptographic software library which is supplied to customers as a basis for their own development, this software function was certified by the BSI (Federal Office for Information Security) in Germany. No mathematical weaknesses were known, nor have been discovered during the certification processes.

安全認證範例

- CNS 27001
  - A.10 密碼學
    - A.10.1 密碼式控制措施
    - 目標：確保適當及有效使用密碼學，以保護資訊之機密性、鑑別性及/或完整性。
      - A.10.1.1 使用密碼式控制措施之政策
        - 控制措施
        - 應發展及實作政策，關於資訊保護之密碼式控制措施之使用
      - A.10.1.2 金鑰管理
        - 控制措施
        - 應發展及實作政策，關於貫穿其整個生命週期之密碼金鑰的使用、保護及生命期

安全認證範例

- 美國國家標準局密碼模組安全要求（FIPS 140-1）
- “While the security requirements specified in this standard are intended to maintain the security provided by a cryptographic module, conformance to this standard is not sufficient to ensure that a particular module is secure.”

（即便本標準所指定之安全要求，用意在保持密碼模組所提供之安全性，符合本標準並不足以確保某一持定模組之安全性）

- 關於密碼模組開發之安全要求
  - 第一安全層級需三份文件、第二層級需一份、第三層級要求軟硬體以高階語言撰寫、第四層級需四份文件加上程式註解

結語

- 密碼系統與密碼程式不同。
- 學術及產業界經由公開檢視以增強密碼系統與程式之安全。
- 現行健康保險資料庫不公開加密方式，無法檢視其安全性。
- 不公開密碼系統及程式，往往造成安全的假象，易造成安全漏洞。
- 安全認證只能有形式上的資訊安全，並非實質上的資訊安全。
- 健康保險資料庫中包含大量民眾個人資訊，其密碼系統及程式之安全性，應以更高之標準檢視。