高校应用数学学报
2022, 37(4): 426-430

一次一密理论的再认识

陆成刚[1], 王庆月[2]

(1. 浙江工业大学 理学院, 浙江杭州 310023;
2. 宁夏理工学院 计算机学院, 宁夏石嘴山 753000)

摘 要: 该文从概率论角度推导了一次一密方法的完善保密性, 进一步在特定条件下推导出明文分布的等概率特性. 此外, 基于信息熵理论证明了在去掉一次一密的密钥分布等概率性条件后仍可以满足完善保密性, 并建议密钥分布等概率性条件对信源压缩编码后的明文的适用性.

关键词: 一次一密; 完善保密性; 信息熵; 等概率性
中图分类号: O175.14
文献标识码: A **文章编号**: 1000-4424(2022)04-0426-05

§1 引 言

1882年银行家弗兰克-米勒首次发现使用了一次性密码本[1], 通信工程师吉尔伯特-佛纳于1919年被授权了也许是密码史上最重要的一个关于一次一密的专利[2]. 克劳德-香农在1940年代发现并证明了一次一密方法的理论意义, 他的报告于1949年被公开[3]. 几乎同时期苏联数学家弗拉基米尔-科特尔尼科夫独立地证明了一次一密的绝对安全性[4]. 王勇提出了密钥分布等概率性与明文概率分布不兼容的问题[5]. 雷凤宇证明了完善保密性密码体制的条件和存在性[6]. 本文重新审视了密钥等概率性条件和满足完善保密性的关系, 在一个特定的完善保密性角度下推导出明文分布的等概率性. 进一步, 传统一次一密理论的密钥等概率性条件可以去掉, 只保留明文和密钥的互相独立性就能证明完善保密性. 这个结果进一步推广了一次一密方法的适用范围, 同时指出密钥等概率特性下的一次一密法仍可以适用于信源压缩编码后的明文加密.

§2介绍一次一密法, §3使用概率论证明了它满足完善保密性, 并且推导出明文的等概率分布特性. §4使用明文和密钥互相独立作条件证明了完善保密性.

§2 一次一密

考虑有限加法群G, 明文, 密钥和密文分别是以G作为样本空间的离散随机变量M, K和C, 并且在每一个样本点上的概率值都大于零. 对明文随机变量M的任一取值m, 令任一密钥k(密钥

收稿日期: 2021-04-18 修回日期: 2022-08-04
基金项目: 宁夏自然科学基金(2020AAC03278); 浙江省重点研发计划: 2022年度“领雁”研发攻关计划(2022C01084)

随机变量K的取值)与之运算得到密文c(密文随机变量C的取值), 即$m+k=c$, 其中+为G中的加法运算. 而解密运算$c-k=m$, $-$为加法运算的逆运算. 明文和密文之间的运算$k=c-m$可以解出密钥. 一个加密算法, 其对应的解密算法和确定密钥的算法决定了三个随机变量M, K和C的三组确定映射

$$\begin{aligned} C &= f(M, K), \\ M &= g(C, K), \\ K &= h(M, C). \end{aligned} \tag{1}$$

其中f为加密函数, g为解密函数, h可由明文和密文确定密钥, 这三个函数是确定的, 已知的函数. 一次一密的主要实现方式为将加密看作一个过程, 则明文序列为与随机变量M同分布的一个随机过程, 每次加密参与的密钥视作与K同分布的一个随机过程. 在K与M互相独立, 并且K的分布为等概率分布(均匀分布)的条件下可以证明一次一密满足完善保密性.

§3 满足完善保密性

见诸于文献的完善保密性主要是指明文与密文互相独立, 即

$$P(M) = P(M|C)$$

或

$$P(M = m) = P(M = m|C = c). \tag{2}$$

它的密码学含义可以解释为知道密文并不能改善对于明文的认识, 即密文没有提供对明文的任何信息. 使用信息熵的语言, 以密文作条件的明文熵等于明文熵, 从而知道明文, 密文的互信息为零, 即

$$P(M)=P(M|C) \implies H(M)=H(M|C) \implies I(M;C)=H(M)\text{-}H(M|C)=0.$$

另外一种常见的完善保密性的定义为

$$P(f(m_1, k_1) = c) = P(f(m_2, k_2) = c). \tag{3}$$

它的密码学意义也很容易理解, 就是密文c是由明文密钥对(m_1, k_1)生成而成还是由(m_2, k_2)加密而成的可能性没有差异. 这个定义等价于联合条件概率分布$P((M, K)|C=c)$为等概率分布.

定理1 以加法有限群G为样本空间的随机变量M, K和C满足f, g和h确定函数组成的式(1), 随机变量M, K互相独立, 随机变量K 概率分布符合均匀分布, 则随机变量M, C满足式(2).

证 设明文m, 密钥k和密文c满足

$$\begin{aligned} c &= f(m, k), \\ m &= g(c, k), \\ k &= h(m, c), \end{aligned} \tag{4}$$

则

$$1 = p(C = c|(M = m, K = k)) = \frac{p(M = m, K = k, C = c)}{p(M = m, K = k)} =$$

$$\frac{p(K = k|(M = m, C = c))p(M = m, C = c)}{p(M = m, K = k)}$$

$$= \frac{p(M = m, C = c)}{p(M = m, K = k)} = \frac{p(M = m)p(C = c|M = m)}{p(M = m)p(K = k)} = \frac{p(C = c|M = m)}{p(K = k)},$$

得到

$$p(C = c|M = m) = p(K = k). \tag{5}$$

其次

$$p(C = c) = \sum_{m' \in G} p(C = c, M = m^{'}) = \sum_{m' \in G} p(C = c|M = m^{'})p(M = m^{'})$$

$$= \sum_{m' \in G, k' = h(m', c)} p(K = k^{'})p(M = m^{'}) = p(K = k) \sum_{m' \in G} p(M = m^{'}) = p(K = k).$$

上面倒数第三个等号利用式(5), 倒数第二个等号利用了随机变量K的概率分布符合均匀分布的特性, 最后的等号说明密文也符合等概率分布,

$$p(C = c) = p(K = k). \tag{6}$$

最后

$$p(M = m|C = c) = \frac{p(M = m, C = c)}{p(C = c)} = \frac{p(C = c|M = m)p(M = m)}{p(C = c)} =$$

$$\frac{p(K = k)p(M = m)}{p(C = c)} = p(M = m).$$

以上倒数第二个等号利用了式(5), 最后一个等式利用了式(6), 这里说明了M, C的互相独立性, 即

$$p(M = m|C = c) = p(M = m). \tag{7}$$

定理2 以加法有限群G为样本空间的随机变量M, K和C满足f, g和h确定函数组成的式(1), 随机变量M, K互相独立, 随机变量K 概率分布符合均匀分布, 当变量M, K和C满足式(3)定义的完善保密性时, 明文一定符合均匀概率分布.

证 由于随机变量M, K互相独立, 随机变量K概率分布符合均匀分布, 由定理1的证明过程得到式(5), (6)成立, 考虑

$$p((M = m, K = k)|C = c) = \frac{p(M = m, K = k, C = c)}{p(C = c)} =$$

$$\frac{p(K = k|(M = m, C = c))p(M = m, C = c)}{p(C = c)} =$$

$$\frac{p(M = m, C = c)}{p(C = c} = \frac{p(C = c|M = m)p(M = m)}{p(C = c)} = \frac{p(K = k)p(M = m)}{p(C = c)} = p(M = m),$$

得到

$$p((M=m,K=k)|C=c)=p(M=m). \tag{8}$$

而式(8)左端是等概率分布的(满足式(3)的完善保密性), 于是右端表明明文也是符合等概率分布的.

§4 新条件下满足完善保密性

为保证完善保密性, 在定理1中设置了一个先决条件, 即密钥的等概率分布特性, 实际上这个条件是冗余的, 下面通过定理3证明在没有这一条件时一次一密方法能够保证完善保密性.

定理3 以加法有限群G为样本空间的随机变量M, K和C满足f, g和h确定函数组成的式(1), 随机变量M, K互相独立, 则随机变量M, C满足式(2).

证 由于式(1)中f, g, h为确定的, 已知算法. 易知以下三条件熵为零

$$H(M|(C,K))=H(C|(M,K))=H(K|(M,C))=0.$$

又

$$H(C,(M|K))=H(C)+H(M|(K,C))=H(M|K)+H(C|(M,K))$$

及

$$H(C,(K|M))=H(C)+H(K|(M,C))=H(K|M)+H(C|(K,M)),$$

得到

$$H(C)=H(M|K)=H(K|M).$$

同理

$$H(K)=H(M|C)=H(C|M).$$

另因随机变量M与K独立, 由$H(C)=H(M|K)=H(K|M)$得到$H(C)=H(M)=H(K)$. 所以$H(M|C)=H(M)$, 进而满足式(2). 此外

$$I(M;C)=H(M)-H(M|C)=H(M)-H(M)=0,$$

说明明文和密文之间的互信息为零, 而这说明明文和密文之间的信道容量为零.

类似在该定理证明中的方法, 可得到

$$H((M,K)|C)=H(M|C)+H(K|(M,C))=H(M|C)=H(M),$$

这说明在$C=c$时, 联合变量(M,K)的不确定性和M是一个量级的, 这也是自然的, 因为M确定了, K自然也确定了. 假如进一步要求满足式(3)的完善保密性, 那么由$P((M,K)|C=c)$的等概率性, 导致$H((M,K)|C)$取到最大值, 即$H(M)$取到最大, 而这实际就是要求明文分布的等概率性. 而定理3说明变量M, K互相独立时, 就可以满足随机变量M, C互相独立的完善保密性, 对明文M的概率分布却没有限制.

此外, 定理3说明在一次一密执行时密钥的等概率性实际是不必要的, 只要密钥与明文独立无关即可. 此外, 在满足特定的完善保密性时, 密钥等概率特性带来了明文分布的等概率特性的

限制, 但这并非对适用的明文产生了制约. 事实上只要明文经过熵压缩信源编码后的码流均能呈现0, 1比特的概率均衡的随机性(如果0, 1出现的概率不均衡, 说明还有进一步可压缩的空间), 这恰恰使得“明文”符合在0, 1比特上的等概率特性. 因此, 在使用密钥等概率特性的一次一密时建议首先对明文进行无损熵压缩编码.

§5 总结与展望

本文重新审视了一次一密的密钥等概率特性与完善保密性的关系, 并通过信息熵工具证明了明文和密钥独立无关条件下的一次一密的安全性. 将来可以考虑信息熵工具用于对公私钥密码体制的安全性分析的研究.

参考文献:

[1] Bellovin Steven M, Frank Miller. Inventor of the one-time pad[J]. Cryptologia, 2011, 35 (3): 203-222.

[2] Gilbert Vernam. U.S. Patent 1,310,719[Z]. https://patents.google.com/patent/US1310719

[3] Shannon Claude. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28 (4): 656-715.

[4] Sergei N Molotkov. Quantum cryptography and V A Kotel'nikov's one-time key and sampling theorems[J]. Physics-Uspekhi, 2006, 49 (7): 750-761.

[5] 王勇. 一次一密的安全性与新保密体制[J]. 信息网络安全, 2004(43): 41-43.

[6] 雷凤宇, 崔国华, 徐鹏, 等. 完善保密密码体制的条件和存在性证明[J]. 计算机科学, 2010, 37(5): 99-102.

Recognition of one-time-one-secret theory

LU Cheng-gang[1], WANG Qing-yue[2]

(1. School of Sci., Zhejiang Univ. of Technology, Hangzhou 310013, China;
2. Dept. of Comput. Sci., Ningxia Polytechnic Institute., Shizuishan 753000, China)

Abstract: This paper derives the perfect secret of the one-time encryption method from the perspective of probability theory, and further derives the equal probability characteristics of the plaintext distribution under certain conditions. In addition, based on the theory of information entropy, it is proved that perfect confidentiality can still be satisfied after removing the probabilistic conditions such as the one-time key distribution, and it is suggested that the probabilistic conditions such as the key distribution are applicable to the plaintext after the source is compressed and encoded.

Keywords: one time one secret; perfect secret; information entropy; equal probability

MR Subject Classification: 94A60