LDPC 码在加密系统中应用的约束条件

林雪红 牛 凯 林家儒
(北京邮电大学信息与通信工程学院 北京 100876)

摘 要：该文首先给出了基于 LDPC 码公钥加密系统中授权用户获取明文的置信传播迭代译码算法，并得出了在明文信息等概的情况下授权用户要成功获取明文，私钥所需满足的必要条件。然后根据置信传播递归迭代算法分析了公钥参数设计的充分必要条件。最后通过仿真验证了私钥和公钥参数设计的正确性。

关键词：LDPC 码；置信传播算法；加密系统
中图分类号：TN911.22 **文献标识码**：A **文章编号**：1009-5896(2010)03-0613-04
DOI:10.3724/SP.J.1146.2009.00160

The Constraint Conditions for LDPC Codes in Cryptosystem

Lin Xue-hong Niu Kai Lin Jia-ru
(*School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

Abstract: This paper first presents Belief Propagation (BP) iteration algorithm in LDPC code-based public-key cryptosystems, and develops the necessary condition of private key if the probability of plaintext is equal. Then the necessary and sufficient condition of public key is deduced according to the recursion of BP iteration algorithm. Simulations show that the parameters of private key and public key are correct.

Key words: LDPC codes; Belief Propagation (BP) algorithm; Cryptosystem

1 引言

纠错码不仅可以抗信道干扰，而且可以用于公开密钥加密系统中。早在 1978 年就已经提出了纠错码的加密方案[1]。基于稀疏校验矩阵定义的线性分组码，即低密度校验(Low Density Parity Check, LDPC)码[2]以其优越的性能和较低的译码复杂度，引起世界各国学术界和 IT 界的高度重视，成为当今信道编码领域最瞩目的研究热点。针对目前 LDPC 码在密码学、信息安全领域的研究主要是分析其安全性和攻击方法[3−6]，但对于授权用户成功解密出明文信息私钥和公钥参数所需满足的条件目前还没有研究，本文给出了授权用户获取明文的置信传播(Belief Propagatio, BP)迭代译码算法，分析了基于 LDPC 码加密系统私钥参数需满足的必要条件和公钥参数需满足的充分必要条件，并通过仿真验证了参数设计的正确性。

2 加密系统

基于一个密矩阵很难分解成几个矩阵的乘积，文献[3]给出了 LDPC 码在公开密钥加密系统中的应用，下面介绍其加解密算法。

2.1 加密算法

设 $\boldsymbol{G}$ 是$(N,\ M)$线性分组码的生成矩阵，且 $\boldsymbol{G}=\boldsymbol{B}^{-1}\boldsymbol{A}\boldsymbol{D}$，其中 $\boldsymbol{D}$ 是维数为 $M\times M$ 的满秩密矩阵，$\boldsymbol{A}$ 和 $\boldsymbol{B}$ 分别是维数为 $N\times M$ 和 $N\times N$ 的稀疏矩阵。其加密算法为

$$E_K(\boldsymbol{s})=\boldsymbol{r}=\boldsymbol{G}\boldsymbol{s}+\boldsymbol{\eta} \tag{1}$$

其中 $\boldsymbol{s}$ 是长为 M 的二进制明文；$\boldsymbol{r}$ 是长为 N 的二进制密文；$\boldsymbol{\eta}$ 是长为 N 的二进制随机序列，且 $P(\eta_i=1)=\mathrm{PB}$，$P(\eta_i=0)=1-\mathrm{PB}$；公钥 $K_{\mathrm{public}}=\{\boldsymbol{G},\mathrm{PB}\}$；私钥 $K_{\mathrm{private}}=\{\boldsymbol{A},\boldsymbol{B},\boldsymbol{D}\}$。

2.2 解密算法

对于非授权用户，需要把矩阵 $\boldsymbol{G}$ 分解成矩阵 $\boldsymbol{A}$，$\boldsymbol{B}$ 和 $\boldsymbol{D}$ 的乘积来进行解密运算。而在分解过程的中，存在多个 3 元组$\{\boldsymbol{A},\boldsymbol{B},\boldsymbol{D}\}$满足 $\boldsymbol{G}=\boldsymbol{B}^{-1}\boldsymbol{A}\boldsymbol{D}$，而且运算复杂度随矩阵 $\boldsymbol{G}$ 的维数呈指数增长，也就是说这种分解运算是不可实现的[3,7]。

对于授权用户根据接收序列 $\boldsymbol{r}$，利用私钥通过以下方法获取明文。

2.2.1 解密步骤 解密过程由如下 3 步完成[3]：

(1)左乘 $\boldsymbol{B}$

$$\boldsymbol{J}=\boldsymbol{B}\boldsymbol{r}=\boldsymbol{A}\hat{\boldsymbol{s}}+\boldsymbol{B}\boldsymbol{\eta} \tag{2}$$

其中 $\hat{\boldsymbol{s}}=\boldsymbol{D}\boldsymbol{s}$。

2009-02-09 收到，2009-09-25 改回
国家 973 计划项目(2007CB310604)和国家自然科学基金(60772108，60702048)资助课题
通信作者：林雪红 lxh121@sina.com

(2)将 $\boldsymbol{J}$ 送入由稀疏矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 级联的矩阵 $\boldsymbol{H}=[\boldsymbol{A}\,|\,\boldsymbol{B}]$ 所构成的译码器执行置信传播(BP)译码算法，得到 $\hat{\boldsymbol{s}}$；

(3)左乘 $\boldsymbol{D}^{-1}$，得到明文 $\boldsymbol{s}$，即

$$\boldsymbol{s}=\boldsymbol{D}^{-1}\hat{\boldsymbol{s}} \tag{3}$$

2.2.2 BP 译码算法 令 $\boldsymbol{H}=[\boldsymbol{A}\,|\,\boldsymbol{B}]$，$[x_1\ \cdots\ x_M]=\hat{\boldsymbol{s}}$ 和 $[x_{M+1}\ \cdots\ x_{M+N}]=\boldsymbol{\eta}$，即式(2)的译码过程等效为根据序列 $\boldsymbol{J}$（$\boldsymbol{J}=\boldsymbol{H}\boldsymbol{x}$）求序列 $\boldsymbol{x}$。定义 $A(m)=\{n:\boldsymbol{A}_{mn}\neq 0\}$ 表示矩阵 $\boldsymbol{A}$ 中与校验节点 m 相连的比特节点，$B(m)=\{n:\boldsymbol{B}_{mn}\neq 0\}$ 表示矩阵 $\boldsymbol{B}$ 中与校验节点 m 相连的比特节点，$M(n)=\{m:H_{mn}\neq 0\}$ 表示所有与比特节点 n 相连的校验节点 $A(m)\backslash n(B(m)\backslash n)$ 表示 $A(m)$（$B(m)$）中除去比特节点 n，$M(n)\backslash m$ 表示 $M(n)$ 中除去校验节点 m；q_{mn}^{i} 表示除校验式 m 以外的其他校验式可信度信息已知的条件下，比特节点等于 i 的概率；r_{mn}^{i} 表示假设比特节点为 0/1 条件下，其他参与校验节点 m 的比特节点提供给校验节点 m=i（也就是满足校验式 m）的概率。

设 $P(\hat{s}_i=1)=\mathrm{PA}$，$P(\hat{s}_i=0)=1-\mathrm{PA}$，则 BP 译码算法包括以下步骤：

步骤 1 初始化

对每个比特节点 $n=1,\cdots,M+N$，令

$$q_{mn}^{i}=f_n^{i}=\begin{cases}\mathrm{PA}\delta_{i,1}+(1-\mathrm{PA})\delta_{i,0}, & n=1,\cdots,M\\ \mathrm{PB}\delta_{i,1}+(1-\mathrm{PB})\delta_{i,0}, & n=M{+}1,\cdots,N{+}M\end{cases} \tag{4}$$

其中，当 $a=b$ 时 $\delta_{a,b}=1$，否则 $\delta_{a,b}=0$

步骤 2 迭代过程

(1)校验节点更新 设 $\delta q_{mn}=q_{mn}^{0}-q_{mn}^{1}$，对每个校验节点 $m=1,\cdots,N$ 和 $n\in N(m)$，计算

$$\delta r_{mn}=\begin{cases}\prod\limits_{n'\in A(m)\backslash n}\delta q_{mn'}\cdot\prod\limits_{n'\in B(m)}\delta q_{mn'}, & n{=}1,\cdots,M\\ \prod\limits_{n'\in A(m)}\delta q_{mn'}\cdot\prod\limits_{n'\in B(m)\backslash n}\delta q_{mn'}, & n{=}M+1,\cdots,M+N\end{cases} \tag{5}$$

$$r_{mn}^{i}=\frac{1}{2}\left(1+(-1)^{i+J_n}\delta r_{mn}\right)$$

(2)比特节点更新 对每个比特节点 $n=1,\cdots,M+N$ 和 $m\in M(n)$，计算

$$q_{mn}^{i}=\alpha_{mn}f_n^{i}\prod_{m'\in M(n)\backslash m}r_{m'n}^{i} \tag{6}$$

对每个比特节点 $n=1,\cdots,M+N$，计算

$$q_n^{i}=\alpha_n f_n^{i}\prod_{m'\in M(n)}r_{m'n}^{i} \tag{7}$$

其中 α_{mn} 和 α_n 均为归一化因子。

步骤 3 尝试判决

根据判定条件：当 $q_n^1>0.5$ 时，$\hat{x}_n=1$；否则，$\hat{x}_n=0$，得到码字 $\hat{\boldsymbol{x}}=(\hat{x}_1,\cdots,\hat{x}_{M+N})$。若满足以下两个条件之一停止译码：(1) $\boldsymbol{H}\hat{\boldsymbol{x}}=\boldsymbol{J}$，$\hat{\boldsymbol{x}}$ 作为有效译码值输出；(2)达到预定的迭代次数，计算误码率。否则，返回步骤 2 开始下一轮迭代。

由于式(2)中的等式关系与 LDPC 码校验关系稍有不同，因此与文献[8]中的置信传播算法相比，该算法的主要不同点是式(5)。

3 加密参数设置

3.1 私钥 $\boldsymbol{A}$ 矩阵的设计

定理 1 若明文信息等概时，即 PA = 1/2，则基于LDPC码的加密系统私钥参数矩阵 $\boldsymbol{A}$ 中至少有一行仅存在一个非零元素。

证明 用反证法。

假设矩阵 $\boldsymbol{A}$ 的每一行都有一个以上的非零元素，即集合 $A(m)$ 中元素的个数大于 1。若明文中的比特信息等概时，则对所有比特节点 $n'\in\{1,\cdots,M\}$，$\delta q_{mn'}=0$，由于 $A(m)$ 中元素的个数大于 1，因此对每个校验节点 $m=1,\cdots,N$，$r_{mn}^{i}=1/2$。由式(6)可知，$q_{mn}^{i}=f_n^{i}$。即随着迭代次数的增加，比特节点 n 不能从其他的比特节点获得附加信息。换句话说，在该校验节点没有信息的传递，使得这种译码算法针对等概的明文不能有效译码。

因此，要使BP译码算法有效，必须满足矩阵 $\boldsymbol{A}$ 中至少有一行仅存在一个非零元素。 证毕

3.2 加扰噪声门限

设 LDPC 码稀疏矩阵 $\boldsymbol{H}$ 由稀疏矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 级联而成，即 $\boldsymbol{H}=[\boldsymbol{A}\,|\,\boldsymbol{B}]$，则该矩阵的比特节点和校验节点可表示为

$$\lambda^{A}(x)=\sum_{i=1}^{d_v^A}\lambda_i^{A}x^{i-1},\quad \lambda^{B}(x)=\sum_{i=1}^{d_v^B}\lambda_i^{B}x^{i-1},$$

$$\rho^{A}(x,y)=\sum_{i=1}^{d_c^A}\sum_{j=1}^{d_c^B}\rho_{i,j}^{A}x^{i-1}y^{j},$$

$$\rho^{B}(x,y)=\sum_{i=1}^{d_c^A}\sum_{j=1}^{d_c^B}\rho_{i,j}^{B}x^{i}y^{j-1}$$

式中 d_v^{Φ} 和 d_c^{Φ} 分别表示稀疏矩阵 $\boldsymbol{\Phi}=\{\boldsymbol{A},\boldsymbol{B}\}$ 中比特节点和校验节点的最大度数；λ_i^{Φ} 表示稀疏矩阵 $\boldsymbol{\Phi}=\{\boldsymbol{A},\boldsymbol{B}\}$ 对应Tanner图上度为 i 的比特节点占所有边的比例；$\rho_{i,j}^{A}$（$\rho_{i,j}^{B}$）表示稀疏矩阵 $\boldsymbol{H}$ 对应Tanner图上度为 $i+j$ 的校验节点（i 条边与 $\boldsymbol{A}$ 相连且 j 条边与 $\boldsymbol{B}$ 相连)占所有边的比例。

定理 2 若 LDPC 码稀疏矩阵 $\boldsymbol{H}=[\boldsymbol{A}\,|\,\boldsymbol{B}]$ 的比特节点和校验节点服从 λ_i^{A}，λ_i^{B}，$\rho_{i,j}^{A}$ 和 $\rho_{i,j}^{B}$ 分布，且与稀疏矩阵 $\boldsymbol{A}$ 对应的比特节点等于 1 概率为 p^{A}，与稀疏矩阵 $\boldsymbol{B}$ 对应的比特节点等于 1 概率为 p^{B}，

如果

$$(1-p^A)\cdot\lambda^A\left(\frac{1-\rho^A(1-2x,1-2y)}{2}\right)+p^A\cdot\left(1-\lambda^A\left(\frac{1+\rho^A(1-2x,1-2y)}{2}\right)\right)<x$$

且

$$(1-p^B)\cdot\lambda^B\left(\frac{1-\rho^B(1-2x,1-2y)}{2}\right)+p^B\cdot\left(1-\lambda^B\left(\frac{1+\rho^B(1-2x,1-2y)}{2}\right)\right)<y$$

其中 $x\in(0,p^A)$， $y\in(0,p^B)$。则授权用户解密成功的充分必要条件是：公钥 PB 的最大值为 p^B。

证明　在 2.2 节中的采用置信传播算法解密过程等效于将全零码字的前 M 个比特信息通过差错概率为 p^A 的 BSC 信道，后 N 个比特信息通过差错概率为 p^B 的 BSC 信道，得到接收序列 $\boldsymbol{r}$，然后送入稀疏矩阵 $\boldsymbol{H}=[\boldsymbol{A}\,|\,\boldsymbol{B}]$ 进行 BP 译码。

度为 l^A+l^B 的校验节点，其中 l^A 条边与矩阵 $\boldsymbol{A}$ 相连，l^B 条边与矩阵 $\boldsymbol{B}$ 相连，则该校验节点提供给与矩阵 $\boldsymbol{A}$ 相连的某个比特节点等于 1 的概率为

$$q_i^A=\frac{1-(1-2p_i^A)^{l^A-1}\cdot(1-2p_i^B)^{l^B}}{2}$$

则所有校验节点提供给与矩阵 $\boldsymbol{A}$ 相连的比特节点等于 1 的概率平均值为

$$q_i^A=\frac{1-\sum\limits_{l^A,l^B}\dfrac{(l^A+l^B)N_{l^A,l^B}}{E}(1-2p_i^A)^{l^A-1}\cdot(1-2p_i^B)^{l^B}}{2}=\frac{1-\rho^A(1-2p_i^A,1-2p_i^B)}{2}$$

式中 N_{l^A,l^B} 表示 l^A 条边与 $\boldsymbol{A}$ 相连且 l^B 条边与 $\boldsymbol{B}$ 相连的校验节点个数，E 为稀疏矩阵 $\boldsymbol{H}$ 的总边数。

采用 BP 迭代译码算法后，与矩阵 $\boldsymbol{A}$ 相连的比特节点等于 1 的概率的递归公式为

$$p_{i+1}^A=(1-p^A)\cdot\lambda^A(q_i^A)+p^A\cdot(1-\lambda^A(1-q_i^A))=(1-p^A)\cdot\lambda^A\left(\frac{1-\rho^A(1-2p_i^A,1-2p_i^B)}{2}\right)+p^A\cdot\left(1-\lambda^A\left(\frac{1+\rho^A(1-2p_i^A,1-2p_i^B)}{2}\right)\right)$$

式中的第 1 项表示若比特节点接收无差错时，校验节点提供的附加信息为 1 的概率；第 2 项表示若比特节点接收错误，而校验节点提供的附加信息为 0 的概率。

同理可证，与稀疏矩阵 $\boldsymbol{B}$ 对应的比特节点等于 1 的概率的递归公式为

$$p_{i+1}^B=(1-p^B)\cdot\lambda^B\left(\frac{1-\rho^B(1-2p_i^A,1-2p_i^B)}{2}\right)+p^B\cdot\left(1-\lambda^B\left(\frac{1+\rho^B(1-2p_i^A,1-2p_i^B)}{2}\right)\right)$$

若迭代收敛，需满足 $p_{i+1}^A<p_i^A$ 且 $p_{i+1}^B<p_i^B$。即

$$(1-p^A)\cdot\lambda^A\left(\frac{1-\rho^A(1-2x,1-2y)}{2}\right)+p^A\cdot\left(1-\lambda^A\left(\frac{1+\rho^A(1-2x,1-2y)}{2}\right)\right)<x$$

且

$$(1-p^B)\cdot\lambda^B\left(\frac{1-\rho^B(1-2x,1-2y)}{2}\right)+p^B\cdot\left(1-\lambda^B\left(\frac{1+\rho^B(1-2x,1-2y)}{2}\right)\right)<y$$

证毕

4　性能分析

设稀疏矩阵 $\boldsymbol{H}=[\boldsymbol{A}\,|\,\boldsymbol{B}]$ 比特节点和校验节点服从的分布是：$\lambda^A(x)=1$，$\lambda^B(x)=x$，$\rho^A(x,y)=y^3$ 和 $\rho^B(x,y)=xy^2$。根据定理2，图1给出了能正确恢复比特节点信息时，矩阵$\boldsymbol{A}$的比特节点和矩阵$\boldsymbol{B}$的比特节点概率为1的最大值PA和PB之间的关系。从图中可以看出，随着PA的增加，PB的概率减少。对应第2节中的基于LDPC加密系统可知，随着授权用户对明文先验信息的减少，所设置的公钥 PB 值减少。当明文的比特信息为等概时(通常的通信总是假定信息等概发生)，即授权用户无任何先验信息，公钥概率的最大值为0.0394。

图2给出了服从上述分布的稀疏矩阵 $\boldsymbol{H}=[\boldsymbol{A}\,|\,\boldsymbol{B}]$，其中矩阵$\boldsymbol{A}$的维数为 756×252，矩阵$\boldsymbol{B}$的维数为 756×756。序列 $\boldsymbol{x}=[x_1,\cdots x_{252},x_{253},\cdots,x_{1008}]$ 中，前252 bit信息为明文信息，后756 bit信息为随机序列，各比特的概率为 $P(x_k=i)=\begin{cases}\mathrm{PA}\delta_{i,1}+(1-\mathrm{PA})\delta_{i,0},\ k=1,\cdots,252\\ \mathrm{PB}\delta_{i,1}+(1-\mathrm{PB})\delta_{i,0},\ k=253,\cdots,1008\end{cases}$，设 $\boldsymbol{J}=\boldsymbol{H}\boldsymbol{x}$，由已知序列 $\boldsymbol{J}$ 通过2.2.2节的BP译码算法恢复序列 $\boldsymbol{x}$，仿真结果如图2所示。从图中可以看出，当授权用户获取明文先验信息越多，即概率PA的值越小，则在随机序列上的概率可以越大，也就是说所设置公钥PB值可以更大。而且当输出明文信息的输入随机序列PB的值小于图1中的门限值时，能保证明文信息可靠恢复。

5　结论

本文首先给出了基于LDPC码的公钥加密系统中授

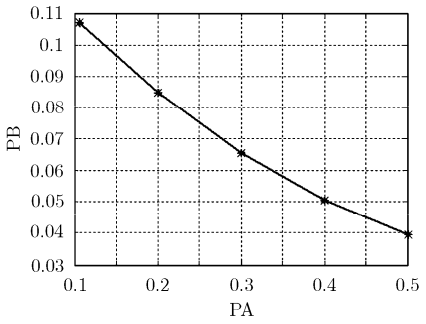

图1 译码成功条件下PA与PB的关系

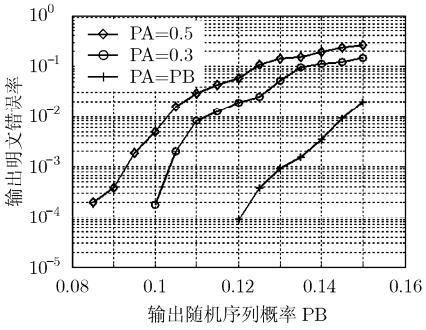

图2 性能仿真

权用户获取明文的置信传播迭代译码算法，并分析了当明文等概时(通常通信中一般假定信息是等概发生的)，私钥需满足的必要条件。然后根据置信传播译码算法的递归迭代过程分析了公钥参数需满足的充分必要条件，即授权用户根据已知明文先验信息的大小，可以确定出具体的公钥参数的值，它随着授权用户对明文先验信息的增加而增加，当无法获取任何先验信息(明文等概)时，所设置的公钥参数 PB 最小。最后本文通过仿真验证了密钥参数设计的正确性。

参 考 文 献

[1] McEliece R J. A public-key cryptosystem based on algebraic coding theory. JPL DSN Progress Report. 1978: 42–44, 114–116.

[2] Gallager R G. Low density parity check codes. *IRE Transactions on Information Theory*, 1962, 8(1): 21–28.

[3] Skantzos N S, Saad D, and Kabashima Y. Analysis of common attacks in public-key cryptosystems based on low-density parity-check codes. *Physical Review E*, 2003, 68 056125.

[4] Baldi M and Chiaraluce F. Cryptanalysis of a new instance of McEliece cryptosystem based on QCLDPC codes. IEEE International Symposium on Information Theory (ISIT 2007), Nice, France, June 2007: 2591–2595.

[5] Otmani A, Tillich J P, and Dallot L. Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes. First International Conference on Symbolic Computation and Cryptography (SCC2008), Beijing, China, April 2008: 1–17.

[6] Fezal A and Sunjiv S. On low density parity check codes for combined reliability and security. AFRICON 2007, Windhoek, Namibia, Sept. 2007: 1–5.

[7] Garey M R and Johnson D S. Computers and Intractability. New York: W. H. Freeman, 1979: 45–76.

[8] MacKay D J C. Good error-correcting codes based on very sparse matrice. *IEEE Transactions on Information Theory*, 1999, 45(2): 399–431.

林雪红： 女，1977 年生，讲师，研究方向为信道编码、MIMO 技术等.

牛 凯： 男，1976 年生，副教授，研究方向为信道编码、MIMO 空时信号处理、无线资源管理.

林家儒： 男，1958年生，教授，研究方向为移动通信、信息处理、编码理论等.